

# Designing Information Systems Security: Interpretations from a British National Health Services Hospital

Gurpreet Dhillon, PhD

Professor of Information Systems, Virginia Commonwealth University

**Abstract-**When designing information systems, an issue of major concern is that control issues are generally considered when user requirements have been abstracted into a logical model. Since such control measures are usually acontextual, they generally lack catalyzing effects that were originally claimed for them. The intent of this paper is to review the logical form of the security measures and the manner in which these have been implemented in a British Hospital. It interprets the ad hoc nature of the security controls and argues that a fuller analysis of organizational contexts is necessary in order to develop secure environments.

## I. INTRODUCTION

Facing pressures of organizational cost containment and external competition, the British National Health Service (NHS) is “rushing headlong” into adopting information technology without careful planning and understanding the security concerns. Individual hospitals are still trying to cope with the intricacy and mystique that surrounds computer systems. It appears that far less security is applied to data held in computer systems than is the case for data held in manual systems. Employees are familiar with the security requirements of a filing cabinet but not necessarily those of an information system [10]. In the NHS, information systems security is generally seen as being of interest to the IT department, and so many professionals do not give adequate importance to these security concerns. Even if they do, they come up with solutions that are over-complicated. Indeed the widespread use of information technology by the health services today has given rise to ‘security blindness’ on part of the users.

In light of such trends, IT managers hold the key to success or failure of a hospital’s well being. In fact the very role of an IT manager is evolving. Organizations can no longer be interpreted in terms of technical installations and their functionality. The focus is shifting so as to consider the ‘wholeness’ and ‘soundness’ of information systems and the organization [8, 2]. Consequently an IT manager is taking on role of maintaining the integrity of the organizational infrastructure (not just the technical information systems). Such a move would minimize the prospect of plagiarism, fraud, corruption or loss of data, and improper use of information systems that could affect the privacy and well being of all concerned.

This paper evaluates the form of the security measures and the means adopted to implement them within a particular hospital setting. It argues that a fuller analysis of organizational contexts is necessary in order to develop secure environments. The discussion is divided into three parts. First analyses the issue of concern with respect to information systems in a particular hospital. Second interprets the form and means of the security measures in place. Third evaluates the implications for practice.

## II. INFORMATION SYSTEMS IN THE HOSPITAL: ISSUES OF CONCERN

The case under consideration looks into a new system that has being introduced into a British NHS Hospital Trust. The Hospital Trust is a specialist one and caters for the needs of people with learning disabilities. The case illustrates the relationship between the design of an IT system and the loss in integrity of the organization and the system itself. Consequently, the new computer-based information system runs a high risk of misuse, abandonment, under-utilization. The case is presented under two headings. First, the wider contextual issues and purpose of the IT infrastructure are discussed. Second, differing interpretations by various stakeholders are discussed. The emphasis is to develop an understanding of the context of the case before discussing the form and means adopted for security.

### A. Purpose of IT infrastructure

In recent years, following contextual pressures, individual hospital trusts in the U.K. have been forced to reassess their information needs. The most conspicuous problem was the timely availability of information. This was particularly the case in the NHS Trust, which is the focus of this study. A computer-based information system was seen as a means to fill this information gap. It was envisaged that such a system would not only help the Trust to adapt to the macro environment (where there was an increased pressure on the Trusts to provide precise information on its activities), but also to add value to the health care delivery process. With respect to the recent changes in the health services, the traditional health care management system had certain shortcomings. For instance it was not possible to give due consideration to isolated ‘encounters’ which could

subsequently be consolidated into health plans. It was also not possible to perform audits and assess the effectiveness of resources used. In response to such criticisms an integrated information system has been implemented at this NHS Trust. It incorporates care-planning functionality in itself and also allows for case mix management and has clinical audit functionality. Thus the system helps the Trust to adapt better to the existing environment. Meeting the demands of the purchasers in providing information to assess the quality and effectiveness of services delivered facilitates this. Such information is drawn through a process of constant monitoring of care delivery, recording of assessment details and measuring of outcomes (refer to figure 1).

In implementing the integrated information system, the Hospital Trust has regarded information technology as

the main catalyst for change. It has relied on IT for successful implementation of the concepts which add value to the health care delivery process and consequently to change the culture of the organization. Little consideration has been given to the systems of responsibility, both formal and informal. Thus there has been an over-reliance on the functionality of the system to reap information technology benefits. As a result the Trust has seen a massive reorganization of its ways of working. The adoption of new management, new structures and new styles of teamwork have come to the forefront. In achieving its objectives the management of the Trust is moving towards adopting principles of systematic monitoring and a single line of command and developing hybrid staff members who know something of everyone's job.

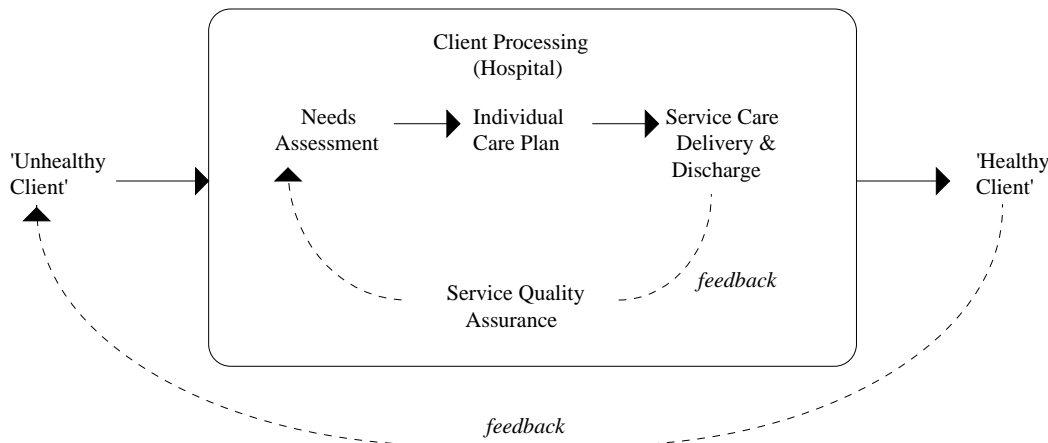


Figure 1, Health care delivery process as perceived by the hospital managers

### B. Interpretations of IT infrastructure

Three professional groups characterize the Trust hospital: clinicians, nurses and managers. The three groups represent their own power structures in the organization. Interviews with members of these groups revealed conflicting ideologies (i.e. organizational and professional ideologies). The doctors and nurses believed in the profession and its norms more than the new goals and objectives being enforced by the new IT infrastructure. The managers on the other hand wanted to derive business value out of the health care delivery process. Though the nurses and doctors agreed with this in principle, they had their own ideas of the manner in which this could be achieved. The doctor's in

particular felt that at a clinical level the system could not be utilized effectively. This was largely because the care-planning module of the system was geared for 'long-stay' patients. The needs of these patients are very different from those who come to the hospital for a 'short-stay' (this is typically the case in psychiatric hospitals). The objective of the information system was clearly in conflict with the organizational policy. The National Health Service in general and the Hospital Trust in particular were striving to move the 'long-stay' patients out into the community. The Trust was also in the process of closing two of its constituent hospitals in the next three years. Thus the need for an over-emphasis on long-stay patients seems unnecessary. The managers, though agreed that patients were being moved out into the community, were not

convinced that the computer-based information system was solely geared for the needs of 'long-stay' patients. Further investigations revealed that in fact the user requirement analysis was flawed. The system developers had been shortsighted in their approach and only the 'long-stay' wards (which were due to be closed in the very near future) had been sampled for requirement analysis.

There is a strong likelihood that the computer-based information system at the Hospital Trust will neither contribute towards enhancing the productivity nor towards the effectiveness of the organization, rather it may make the organization highly vulnerable. This is because there is a mis-match between the actual practices and the formally designed information system. There are two contributing reasons. First, since the organization represents a split hierarchical structure (i.e. between clinicians and managers), the informal organizational norms are very weak, indicating the prevalence of an informal environment where the clinical and business objectives do not support each other. This has resulted in a remarkable difference in roles created by the formal system and as they actually exist. Second, though all stakeholders (doctors, nurses and managers) agreed that ideally the system would be a boon to the organization, there was disagreement on the manner in which it had been developed and implemented. The emergent organizational work practices were technology driven; i.e. it was the computer system that was determining the formal reporting and authority structures. Moreover, it was also forcing unrealistic informal social groupings on to the members of the organization. Since the key players were unhappy with the change process, there is the risk of the information system not being used.

### III. SYSTEMS ANALYSIS WITHIN THE HOSPITAL TRUST

Health care delivery process, although visible, is known to most people at the service delivery level. Some of the elements of service delivery are highly norm based while others follow strict rule structures and are therefore procedure oriented. Within an organization these rules and procedures act as symbolisms producing images and narratives about different events. An interplay of rule and norm based structures determines the patterns of behavior in any given context. In the previous sections we have noted the cultural significance and the meaning content of these rule and norm structures. This section analyses the form and the means in which these rules have been implemented. Ideally, the rules specified for the IT infrastructure should adequately represent the real world of the organization [7]. If this does not happen then the computer based information systems run a high risk of being misused. Security concerns are therefore paramount when considering the implementation or viability of rule structures.

#### A. Logical service specifications at the Hospital Trust

In the particular case of the information system at the Hospital Trust, the system developers and the project team regarded Trust activities as an input-output process. Therefore they considered the health care process in terms of patients coming into the hospital, being treated and then discharged into the community (also depicted in figure 1). This conception helped in modeling the systems development tasks by using the Structured Systems Analysis and Design Methodology (SSADM). The first phase of SSADM, analysis of the current system, identified eleven sub-systems within the hospital environment. These sub-systems interact with each other to transform patients so as to improve their learning skills. The eleven sub-systems are: Admit client; Provide care; Client administration; Resettle client; Contract management; Staff deployment and duty rostering; Pharmacy; Monitor service quality; Provide staff training and development; Budget management; Manage ward. In conducting the analysis of the current system, SSADM requires an analyst to investigate into problems, bottlenecks or dissatisfactions amongst users. This is an important stage since the very success of the final product may depend upon correct requirement assessment. The analysts for the integrated information system were supposedly directed by the Planning Manager to key personnel in each of the functional areas. Discussions with different people revealed that these personnel were not rightly placed to provide the required information to the analysts. Two interesting issues emerge. First, either the Planning Manager purposefully directed the analysts to these individuals or there are doubts about his competence. Second, the analysts (who were outside consultants) should have taken the initiative to define the problem domain adequately. The result of this is that though various processes had been identified, there was no consideration given to user reactions. A careful interpretation of such reactions helps in the development of a rich picture and assesses the pragmatic and semantic aspects appropriately.

The second stage of SSADM provides a logical view of the required system. The system analysts identified five core activities, viz.: Administer client; Provide care; Administer trust; Resettle client; Manage staff deployment. The logical structure was again based on the input-output model. The underlying presumption in this case is that if the needs of individual sub-systems are being met, then the needs of the overall system are also being fulfilled. The logical view of the system has problems at two levels. First, it is based on an inadequate systems requirement, which is an output of the first stage. Second, the control transforms introduced in the DFDs do not represent the real operations. The reason for this is also related to the problems in requirement analysis. Implementation of controls at this stage is a very sensitive issue. These become apparent once the system is automated. Because the nature of logical controls does not match the prevalent structures, there are problems of incoherence. This becomes clear from the structure of the 'Provide Care' sub-system of the

information system. The module is central to the health care delivery process and its successful operation depends on the construction of an individual care plan for each patient. However the analysts do not consider the relatedness of individual care plans and the organizational functions. The formal model for developing an individual care plan is based on the notion of choosing dishes from a hospital menu, a concept that does not consider the needs of the doctors. This notion is related to the ongoing conflict within the Hospital Trust regarding whether an individual care plan is drawn out of a ward round or *vice versa*. Such discordance becomes more obvious in a hospital that provides care to the mentally ill. Individual care plans work well in residential wards, but the management is closing those wards. What would be left will be the acute wards. Consultant doctors within the Hospital Trust are of the opinion that in this new setting primacy cannot be given to individual care plans. Judgments about care plans are largely dependent on ward rounds. In fact they proposed the merger of wards rounds and care plans when considering health care provision for acute wards. The logical model of integrated information system simply considers the existence of a care plan and bases the controls (error handling routines) and security mechanisms around them. The 'Provide Care' module typically is constituted of six processes: assess needs; construct care plan; plan care delivery; review care; monitor care; implement care. Each of the processes gets constant input from the individual care plans for the purpose of monitoring and control. The quality of the logical model can well be imagined since there is an over-reliance on individual care plans, which necessarily do not represent the real world situation.

The second stage of SSADM also looks into the new requirements of the users. These are then included into the logical models. However because of requirements analysis problems such new needs have not been met. In one particular case the requirements of some doctors have simply been ignored. The Hospital Trust is a center of post-graduate training of psychiatrists. The Medical Federation, that provides funding, had requested the consultants of the Trust to develop an IT infrastructure to better manage the training function. The consultants approached the project team in this regard but the planning manager declined to provide any system support in the short term. The consultants could not wait for years for such a system being developed, so they bought some custom software from a vendor. The planning department for a number of reasons should not have ignored such a requirement. First, since it is a user requirement it should have been considered adequately. This would have also prevented independent system developmental activities at the unit or departmental level. Second, inadequate management of the training schemes would affect the quality of the training process, which in turn means that funding may have been withdrawn. This could result in losing accreditation for the training programs resulting in the loss of manpower. Had the system analysts been aware of the consequences, they

would probably have considered this new requirement more sympathetically.

Other stages of SSADM have had problems as well. The final set of formalisms selected by the users also does not represent the real environment. A feasibility study of various options for implementation was carried out and later presented to the users. Two interesting issues emerge. First, the users selected do not represent the real setting of the Hospital Trust. The ward managers involved in the study specialize in long stay residential care and non-acute illnesses. Consequently the focus of the information system is skewed in that direction. Second, the residential non-acute specialties are being relocated from hospitals to a community setting. The requirements in the new environment will be substantially different from what they are at present. The system developers have not considered this aspect. The reason is that none of the users from the acute mental illness units have been involved in selecting options for the system. The underlying intentions for such a situation are more political than indiscreet. Had the system analysts been aware, consideration would have been given to these factors. The remaining stages of SSADM though having been carried out adequately are insufficient because of inconsistency problems highlighted above.

### *B. Logical control measures*

It is a well documented fact that prior to system development, designers should achieve a deep understanding of the application problem domain [6,3]. In terms of developing secure systems, it is important that security features are considered along with the system design process [5]. Accordingly Baskerville identifies three distinct stages. First, the emphasis should be to produce the right kind of security rather than implement security correctly. If latter is the case, then security is being considered as an after thought to systems development. Second, either logical or transformational models should characterize security design in itself<sup>1</sup>. Third, rather than emphasizing cost-benefit risk analysis, the focus should be on the usage of abstract models. Though there is a limited effort in using these concepts, the SSADM-CRAMM<sup>2</sup> interface offers some opportunities.

The system development team at the Hospital Trust, which used both SSADM and CRAMM, has however failed to capitalize of the benefits of the SSADM-CRAMM interface. As of now CRAMM is the only risk analysis method that has been integrated into the overall information systems design and development. The method comprises three

---

<sup>1</sup> Logical models consider the needs of a system in a data-oriented (functional) manner. The transformational models emphasise more on the organisational and behavioural needs. System development for the information system at the Hospital Trust is based on logical modeling.

<sup>2</sup> CRAMM is the CCTA risk analysis methodology

stages, each being supported by the CRAMM software<sup>3</sup> [11].

- Stage 1, sets up the scope and boundary of the analysis. Owners of the data are identified and interviews conducted.
- Stage 2, groups the organisational assets logically by using a database of generic threats.
- Stage 3, suggests countermeasures on basis of asset groups, risk levels etc. (see figure 2).

The main difficulty of using CRAMM is the level of expertise expected from the analysts in carrying out stages 1 and 2 [15]. Used properly CRAMM accepts inputs from different stages of SSADM. Stage 1 of CRAMM proposes a set of countermeasures based on the initial system specifications. The second review stage produces a set of countermeasures based on the initial view of data and the business options as conceived by the analysis and requirements specification stages of SSADM. The third stage identifies countermeasures on the basis of the technical decisions taken while using SSADM. A final list of countermeasures is generated which is later used in the physical design of the system.

In the Hospital Trust information system, the emphasis in generating countermeasures has been skewed towards stage 3 of CRAMM. Rather than using inputs from SSADM to identify countermeasures at stages 1 and 2 of CRAMM the systems developers have used the NHS Management Executive’s documentation to identify broad categories of threats. An important step in stage 1 of a CRAMM review is the identification of ‘data owners’ and then conducting qualitative interviews with them for asset evaluation. This has not been done. Interviews were conducted only with the Chief Executive, the Planning Manager, the IS Manager, Director of Finance, the Administration Manager in one of the constituent hospitals and the Medical Audit Manager. A few members of the system user group who did participate gave more information suitable for system development activities rather than for asset evaluation. Moreover the interviewees are not necessarily the ‘data owners’.

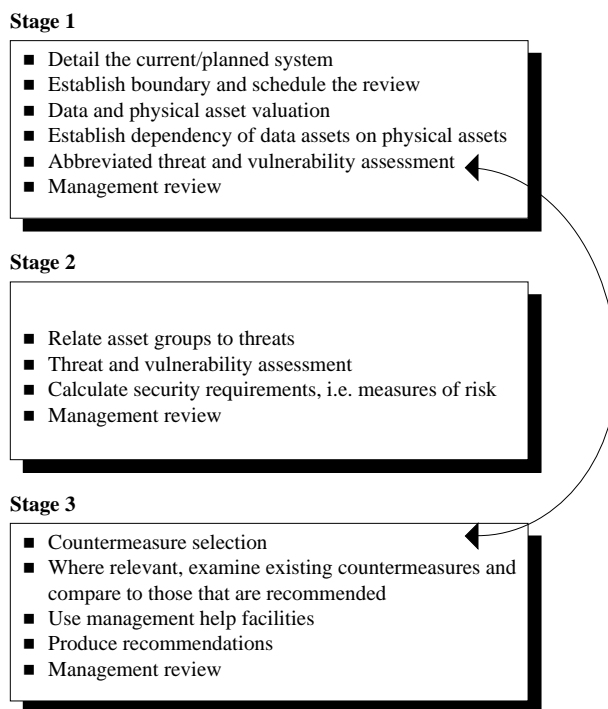


Figure 2, Overview of CRAMM

The notion of identifying ‘data owners’ is complex in itself. This concept is based on the presumption that almost “everything in existence on the earth ‘belongs’ to some individual or organization”[9]. Therefore an owner of an asset has authority over it and has responsibility for its safekeeping. This assumption facilitates the implementation of control mechanisms in a strictly hierarchical manner. The origins of such a notion can probably be traced to the military sector, where there is a prevalence of strict hierarchies and it is relatively easy to delineate data into concrete physical entities. However in a civilian environment, identifying responsible agents may not be all that easy. This is more so in a hospital setting which is gradually evolving into an organismic form (i.e. it is developing strong external relationships and weak internal structures).

In Hospital Trust, though the analysts used CRAMM to identify possible countermeasures so as to establish relevant controls in the physical design phase, they did not carry out the tasks suggested in stages 1 and 2. The complexities, problems and shortcomings in identifying ‘data owners’ and valuing assets are marginalized when CRAMM itself is not used correctly.

### C. Structure of the controls

The means of implementing security controls are as dubious as the form of the controls. This becomes clear on analyzing the existing control mechanisms at Hospital Trust’s information system. The analysis can be performed by

<sup>3</sup> Of late CRAMM has been a subject of lot of criticism; therefore CCTA has commissioned a research and development project which culminates in the release of a new version later in 1995.

looking at processes and the related modulators<sup>4</sup>. A simple example is the process of recording someone's fingerprint. An impression must be left on a greasy surface, glass or special paper before being observed by the human system. In this case modulation concerns the manner in which a signal is given some physical representation before being observed. This interpretation is a two way process. Not only can an object leave an impression (finger print - a sign) for interpretation, but also a number of signs can be translated into a physical object. Control is instituted through a feedback process, the emphasis being on having a minimal level of departure from desired performance. An adequate control therefore is the one in which the 'modulator' retains the meaning of the final outcome.

The controls in the information system can be analyzed by looking at the characteristics of the modulation process. Consider the Client Care module of the system. Doctors diagnose and analyze the patients' requirements through a complex set of signals, even though they are observing a single modulation process. The meaning of their final prognosis depends heavily on the relationship with patterns formed with other signals. The module however is 'straight-jacketed' and does not allow subjective interpretations. Typically it permits a doctor/nurse to enter the goal of the treatment, expected outcome and the desired outcome. Additionally there is a facility to prioritize the goals. The controls emphasize on the efficiency of service delivery, giving no consideration to outside influences. The controls are implemented with the assumption that inputs and outputs of the modulator (the rule structure of the information system in this case) can adequately be captured and assessed. Furthermore it is assumed that the primary source of a given data will go in as input to the system and that the output is a result of a convenient recording operation. The doctor or a nurse can then see the deviations in performance, which can subsequently be rectified. The mechanisms are represented diagrammatically in figure 3.

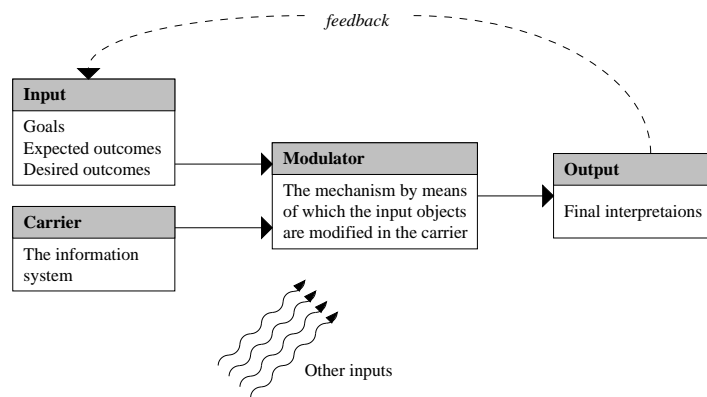


Figure 3, The control feedback loop and the emergent concerns

If we take a real life example of a patient coming into hospital for treatment, the simplistic control structures of the module become obvious. An initial review of the patient may indicate symptoms of some kind of *Schizophrenic psychosis* but it may require considerable effort to pinpoint the class of schizophrenia. Since the goal, expected outcome and desired outcome can not be stated as clearly as the system expects us to do, the very use of the module becomes questionable. In terms of modulation the origins of the problem can be traced to the influences of other signals onto the modulator. In the particular instance of diagnosing *Heberphrenia*, a class of *Schizophrenic psychosis*, the other signals take the form of symptoms such as 'shallow mood accompanied by giggling', 'self absorbing smile', 'hypochondriacal complaints' etc. The final interpretation of a doctor is therefore very different from the perceived outcomes. The system attempts to impose a strict formal control of comparing the output to the input without considering the complexity of the task. The existence of such controls is very problematic and raises concerns for security, particularly that of misinterpretation of data. This can be a serious security concern.

#### IV. SUMMARY

The health care delivery process as conceived and conceptualized by the managers of the Hospital Trust has subsequently been translated into a computer-based information system. Ideally the computer-based system should link the understanding and expression of ideas to the formal systems [13]. This should form the basis for generic solutions around which specific applications can be built. Liebenau & Backhouse [13] identify the notion of 'usage' and 'reference' as fundamental to establishing a link between the intentions and meanings (i.e. semantic considerations) and the formal representations (i.e. syntactical issues). 'Usage' refers to the ways in which formalisms are created and the concept of 'reference' links the formalisms to actual actions. Table 1 which summarizes the security concerns for each module of the information

<sup>4</sup> The basic ideas of modulation are rooted in Shannon's Mathematical Theory of Communication. The notion assumes that when a message is communicated it gets translated while moving from one medium to another. In doing so it carries a set of patterns from one medium and imposes them onto another.

system, links these to an inadequate understanding of the 'usage' and 'reference' issues by the system analysts.

Considering the computer based systems development activities, the various modules of the integrated system represent the formalisms, which encompass the elements of health care delivery process. The actual delivery of services is related to functionality of the modules. In a good systems development activity, the correct use of 'usage' and 'reference' concepts is very important since it allows us to relate meanings of our actions in the real world to actual physical, social and legal operations. Ideally, the rules specified for the IT infrastructure should adequately represent the real world of the organization [7]. This has not

been achieved in the integrated information system at the Hospital Trust. Part of the problem lies with the kind of methodology chosen for systems development, i.e. SSADM (Structured Systems Analysis and Design Methodology). Although SSADM helps in mapping the requirements of the manual system, it is rather difficult to generate a 'rich picture' of the organization. Consequently, the rules and procedures of the information system ignore power, politics, intentionality and beliefs of different individuals and groups. The system developers lack a clear understanding of the 'real world' resulting in an inadequate system being developed which runs a high risk of under utilization or even complete abandonment.

<b>Modules</b>	<b>Issues regarding nature of the formalisms ('usage')</b>	<b>relationship of formalism to actions ('reference')</b>	<b>Security concerns</b>
Administer Client	Translates the whole manual operation into a computer based one	The module relates to the actual practices	Though primary concern is for privacy that can be maintained by password protection, there are however implementation problems
Provide Care	Presumes that patient needs can easily be categorized and hence imposes predetermined classes of activities	Computer based classes do not adequately represent the 'real world' actions	Problem of validity of perceived actions. Because of such inconsistency problems even simple control mechanisms run the risk of being misused/not used
Manage Pharmacy	Translates pharmacy record maintenance onto the computer	Falls short of fulfilling the basic objective of pharmacy costing and drug utilization reviews	Threats of vulnerability to competitors and integrity problems of the pharmacy processes
Administer Trust	Formal structures of this module presume that all other modules are being used adequately	Logically the module would generate relevant management information	Because this module draws information from 'provide care' and 'resettle client' modules, its success depends on those modules
Resettle Client	Module based on the premise: <i>minimize patient stay in the hospital</i>	A worrying trend because it questions the significance of managerial jobs. This has prompted managers to reassess their objective	The information system attempts to be a medical decision support system. Validity of such systems is questionable. Raises problems of power and conflict
Manage Staff Deployment	Computerizes the personnel aspects: wages, salaries, duty roistering etc	No emphasis on training and development - a real requirement	Excessive personnel controls result in alienating employees

Table 1, Summary of the form of the information system and related security concerns

## V. IMPLICATIONS FOR PRACTICE

The analysis of the form and means of the security measures indicated concerns with the design and development of computer based information systems. Design and development is a social process that encompasses communication, learning and negotiation between different stakeholders in an organization [16]. The process draws upon structured methodologies as a means to accomplish the design and development tasks. The methodologies evaluate the problem domain by either taking a technical and an objective view of the phenomena or are more subjective in interpreting the issues. Since security design methods are rooted deep in the systems design methods they may in turn take a subjective or an objective orientation. However, the question that is often asked is that do we need a separate security design methodology or the existing systems design methodology are sufficient? The analyses of findings of this research indicate that indeed security can be integrated into the existing systems analysis and design approaches. The emphasis however should be less on the technical, programmable aspects and more on the requirements elicitation and specification criteria. Doing so will produce a system that is comprehensive, correct and complete. This is clearly illustrated in the form and means of security measures in the Hospital Trust. Having developed a good quality system would implicitly mean that it has a good security design. Such beliefs form the basis of some fundamental principles, adherence to which would determine the integrity of the designs. These are discussed below.

### A. Principles

#### 1. A deeper understanding of the organizational environment should form the basis for security designs.

Since systems development and security designs relate to shaping of new forms of identity at work, new social structures and new value systems, an understanding of the deep seated cultural aspects of a system would allow an appropriate security design. However, the choice of systems development methods and respective security designs is often determined by the mindset of the people involved and immediate economic and social pressures on an organization. In this case it is worthwhile to know the limitations and of the respective choices so that the overall quality of the systems is maintained.

Most of the existing approaches to systems development and security are rooted in functionalist thinking that purports ahistoric and non contextual controls to be implemented. The systems design in itself is based on isolating dependent and independent variables from their contexts. Consequently the designs and the related controls are not situational, holistic and emergent. Other approaches may be grounded in objective view of the world. Objectivity by itself is not criticized here, but since the emphasis is to institute controls by giving primacy to the mechanics of

socio-economic structures there is a significant element of determinism in doing so. The most suitable approach, and the one propounded in this paper, is contextualist in nature. Thus in developing systems and instituting controls, primacy is given to realism of context and theoretical and conceptual development as the primary goal [14].

#### 2. Good security design will lay more emphasis on 'correctness' during system specification.

Correctness in system specification is the key to a good security design. However, system developers and researchers alike have had varying degrees of success in proposing mechanisms, which would facilitate the development of appropriate systems. There have been attempts to take the 'best' aspects of various approaches so as to extend the usefulness of the methodologies. Avison & Fitzgerald [4] however note that doing so may result in the whole breadth of information systems development lacking a coherent philosophical base.

In order to specify systems that are 'correct', it is useful to distinguish between the human information communication functions and the technology platform needed to carry out such processing. The underlying belief here being that an organization in itself is an information system, which allows human agents to communicate with each other resulting in purposeful activity. In this case a system specifier should first address the social issues related with beliefs and expectations of different people, their culture and the value system. Next the intentionality and communications of various agents needs to be analyzed. Developing an understanding of the different meanings associated with the action follows this. Such an interpretation provides an analyst with a deep understanding of the organizational issues and facilitates decision making about what aspects can best be supported by technology. There are no discrete steps to arrive at such a decision; the process is interpretive and contextually motivated. Understanding so gained allows formal specification of the rules and procedures, formal structures and logical connectivity of different modules. These can then be translated into computer programs. The emphasis here is on developing a sound understanding of the deep seated pragmatic aspects of the problem domain. The better an understanding, greater is the probability of achieving 'correctness' in system specifications.

#### 3. A secure design should not impose any controls, but choose appropriate ones based on the real setting.

The preoccupation of most system developers with respect to implementing controls is with 'what ought to be, rather than what actually is'. This flows from the assumption that there is only one best way to organize elements of a system. In such a situation prescriptive recommendations are made and a system is expected to behave in a predetermined manner. In fact control is "the use of interventions by a controller to promote a preferred behavior of a system-being-controlled" [1]. In that sense, a control refers to a broad range of interventions. Such interventions relate to composition and

modification of the tasks of individuals or groups, increase or decrease in the formal rules and procedures or changes in management practices related to training and education. In practice controls do not always prove the desired results. Therefore it's important to evaluate the context in which a controls will be implemented.

With respect to systems analysis and design, a major threat is that control issues are generally considered when user requirements have been abstracted into a logical model<sup>5</sup>. Without having contextual clarity, such controls generally lack catalyzing effects that were originally claimed for them. Leavitt [12], while addressing the issue of organizational change, refers to such 'acontextual' controls as "one-track solutions". These are solutions that are offered for isolated problems without considering other control systems and their contexts. Controls therefore cannot be placed arbitrarily within the design of a system. Implementing system security controls is context driven and should be considered as a major managerial issue.

In conclusion, the evaluation of form and means of security measures in the Hospital Trust have ignored the contextual and the deep-seated pragmatic concerns. This has resulted in dehumanizing the security design and development process. The analysts have brought determinism to the center stage with an endeavor to replace the non-rational qualities of human beings with mechanistic rules of rationality. Indeed, the vain hope has been to develop measures for the level of security and have an objective view of the consequences.

#### REFERENCES

- [1] J. E. Aken. On the control of complex industrial organizations, Nijhoff, Leiden, 1978.
- [2] I. O. Angell. Computer security in these uncertain times: the need for a new approach, Proceedings of the tenth world conference on Computer Security, Audit and Control, COMPSEC, London, UK, pp. 382-388, 1993.
- [3] D. Avison and T. Wood-Harper. Information systems development research: an exploration of ideas in practice, Computer Journal, Volume: 34, Issue: 2, pp. 98-112, 1991
- [4] D. E. Avison and G. Fitzgerald. Information Systems Development: Methodologies, Techniques and Tools, Blackwell Scientific Publications, Oxford, 1988.
- [5] R. Baskerville. Designing information systems security, John Wiley & Sons, New York, 1988.
- [6] R. Baskerville. Information Systems Security Design Methods: Implications for Information Systems Development, ACM Computing Surveys, Volume: 25, Issue: 4, pp. 375-414, 1993.
- [7] P. B. Checkland. Systems thinking, systems practice, John Wiley & Sons, Chichester, 1981.
- [8] G. Dhillon and J. Backhouse. The Use of Information Technology in Organizations: Dealing with Systemic Opportunities and Risks,

Proceedings of the second SISnet Conference, 26-28 September, IESE, Barcelona, 1994.

- [9] P. Dorey. Security management and policy, in W. Caelli, et al. (eds.), Information security handbook, Stockton Press, New York, pp. 27-74, 1991.
- [10] R. Dunn. Data integrity and executive information systems, Computer Control Quarterly, 8, pp. 23-25, 1990.
- [11] B. Farquhar. One approach to risk assessment, Computer Security, Volume: 10, Issue: 1, pp. 21-23, 1991.
- [12] H. J. Leavitt. Applied organization change in industry: structural, technical and human approaches, in W. W. Cooper, et al. (eds.), New perspectives in organization research, John Wiley, New York, 1964.
- [13] J. Liebenau and J. Backhouse. Understanding Information, Macmillan, London, 1990.
- [14] A. M. Pettigrew. Contextualist Research and the Study of Organizational Change Processes, Proceedings of the Research Methods in Information Systems, Manchester, 1985.
- [15] G. Polson. Risk Analysis - a consultants perspective, Proceedings of the 1995 Security Colloquium, Computer Security Research Center, London School of Economics and Political Science, London, January 26, 1995.
- [16] G. Walsham. Interpreting information systems in organizations, John Wiley & Sons, Chichester, 1993

---

<sup>5</sup> Baskerville [5], for example, emphasises the importance of instituting controls in the logical design phase of conventional structured systems analysis and design methods.