Pergamon

0268-4012(95)00062-3

*International Journal of Information Management*, Vol. 16, No. 1, pp. 65–74, 1996
Copyright © 1995 Elsevier Science Ltd
Printed in Great Britain. All rights reserved
0268-4012/96 $15.00 + 0.00

# Risks in the Use of Information Technology Within Organizations

G DHILLON AND J BACKHOUSE

**Information systems researchers and practitioners alike have always felt the need to minimize systemic risks arising out of the use of information technology. Research has identified the confidentiality, integrity and availability of information as vital concepts. However, in developing counter-measures to threats in these three areas the focus has been on questions such as computer viruses, hacking, system failures and access control. Thus the primary concern has been for the technical installations and their functionality. In contrast this research sees information technology usage in terms of the integrity and the wholeness of systems, social as well as technical. It argues that by maintaining the integrity of information systems, the risks associated with information technology usage can be minimized.**

Gurpreet Dhillon is with the Cranfield School of Management, ISRC, Cranfield, Bedford MK43 0AL, UK, Tel: 01234 751122; Fax: 01234 751806; email: g.dhillon@cranfield.ac.uk.

James Backhouse is with the London School of Economics, CSRC, Houghton Street, London WC2A 2AE, UK. Tel: 0171 955 7641; Fax: 0171 955 7385; email: j.p.backhouse@lse.ac.uk.

## Introduction

The benefits of using information technology (IT) in organizations cannot be underestimated. No wonder there has been a dramatic increase in its use. In the UK, by 1993 the overall company expenditure on IT exceeded £15.5 billion.[1] Additional investments have promised huge cost savings. For instance, it is estimated that by implementing information and communication technologies, the British National Health Service could save £300 million per annum.[2] Similarly, the UK Government's Central Unit of Purchasing could save £500 million per year on non-defence purchases.[3] Though cost savings because of the use of IT seem enormous, we must recognize that between 30–40 per cent of the projects realize no net benefits.[4] Besides, nearly 75 per cent of system development projects are either not completed or not used on completion.[5] While wastage in expenditure is a serious problem,[6] the systemic risks ensuing from such endeavours are even more dreadful. Studies have indicated that such problems are not typical of high risk, complex and unstructured ventures, but in fact all types of projects are equally susceptible.[7] This necessitates us to broaden our understanding of risks, not just in economic terms but also organizational and technical.

Against this background of systemic opportunities and risks, organizations are still trying to cope with the mystique that surrounds technology and the myriad benefits that could be derived from it. Furthermore there is reluctance on the part of users to deal with IT related risks.[8] Consequently, far less risk evaluation is done for computer-based systems than is the case for manual paper-based systems.[9] This paper addresses the issues of the risks associated with the

[1] WILLCOCKS, L (1993) *Information Systems in the Public Services: Management Trends and Issues in the United Kingdom* RDP93/7 Oxford Institute of Information Management, Templeton College, Oxford

[2] TOMLIN, R (1991) 'Developing a management culture in which information technology will flourish: how the UK can benefit' *Journal of Information Technology* (6) 45–55

[3] EDI ANALYSIS (1990) 'EDI could help save UK government £500 million a year' *EDI Analysis* 1

[4] WILLCOCKS, L (ED) (1993) *Of Capital Importance: Evaluation and Management of Information Systems Investments* Chapman and Hall, London

[5] EWUSI-MENSAH, K AND PRZASNYSKI, Z H (1991) 'On information systems project abandonment: an exploratory study of organisational practices' *MIS Quarterly* (March) 67–86

[6] HUTCHINSON, W (1994) 'The concept of waste and its use in information system

*continued on page 66*

*continued from page 65*

design' in proceedings of the *1994 International System Dynamics Conference* University of Stirling, Scotland

[7]*Op cit*, Ref 5

[8]BIRCH, D AND MCEVOY, R (1992) 'Risk analysis for information systems' *Journal of Information Systems* (7) 44–53

[9]DUNN, R (1990) 'Data integrity and executive information systems' *Computer Control Quarterly* **8** 23–25

[10]Based on, ANGELL, I (1990) 'Computer security in these uncertain times: the need for a new approach' in *The Tenth World Conference on Computer Security, Audit and Control, COMPSEC* Elsevier Advanced Technology

[11]For example, *op cit*, Ref 8; WILLCOCKS, L AND MARGETTS, H (1994) 'Risk assessment and information systems' *European Journal of Information Systems* **3** (2) 127–139; BASKERVILLE, R (1991) 'Risk analysis: an interpretive feasibility tool in justifying information systems security' *European Journal of Information Systems* **1** (2) 121–130.

[12]FLETCHER, S (1994) 'The risk-based information system design paradigm' in *Tenth IFIP International Symposium on Computer Security, IFIP Sec '94* Curaçao; EKENBERG, L, OBEROI, S AND ORCI, I (1994) 'A cost model for managing information security hazards' in *Tenth IFIP International Symposium on Computer Security, IFIP Sec '94* Curaçao; JAWORSKI, L M (1993) 'Tandem threat scenarios: a risk assessment approach' in *16th National Computer Security Conference* Baltimore, MD, National Institute of Standards and Technology/National Computer Security Center, USA

[13]For example, WILLCOCKS AND MARGETTS, *op cit*, Ref 11; MCFAUGHEY, J R E, SNYDER, C A AND HOUSTON H, C (1994) 'Implementing information technology for competitive advantage: risk management issues' *Information & Management* **26** (5) 273–280

[14]For example, *op cit*, Ref 8; EKENBERG *ET AL*, *op cit*, Ref 12; KAILAY, M AND JARRATT, M (1994) 'RAMeX: a prototype expert system for computer security risk analysis and management' in *Tenth IFIP International Symposium on Computer Security, IFIP Sec '94* Curaçao; ANDERSON, A M, LONGLEY, D AND TICKLE, A B (1993) 'The risk data repository: a novel approach to security risk modelling' in *Ninth IFIP International Symposium on Computer Security, IFIP/Sec '93* Deerhurst, Ontario; SCOTT MORTON, M (ED) (1991) *The Corporation of the 1990s* Oxford University Press, Oxford; EARL, M (1991) *Management Strategies for Information Technology* Prentice-Hall, London; PARKER, M, BENSON, R AND TRAINOR, E (1988) *Information Economics: Linking Performance to Information Technology* Prentice-Hall, Englewood Cliffs; SALTMARSH, T AND BROWNE, P (1983) 'Data processing — risk assessment', in *Advances in Computer*

*continued on page 67*

use of information technology in organizations. It argues that by maintaining the integrity of information systems the risks associated with IT usage can be minimized. Integrity is defined in terms of the 'wholeness' and 'soundness' of information systems. The discussion is based on the premise that minimizing risks is an integrity issue which should lie at the very centre of any corporate strategy.[10] Moreover, risks cannot be evaluated solely by interpreting organizations in terms of technical installations and their functionality. The next section analyses this issue in more detail. This is followed by the findings from two case studies and their discussion.

## The issue

Risks ensuing from the use of IT in organizations have received much attention, both in academic studies and managerial practice.[11] The studies can be classified into two categories. The first category includes research that considers risk management and security of systems as nothing more than dealing with computer viruses, hacking, system failures and access control. Consequently, developing a secure environment means the identification of threats, assessing their probability of occurrence and building respective countermeasures.[12] This group of studies has largely been associated with computer scientists who are concerned with providing complex technological solutions. The second category includes studies by accountants and business managers who evaluate computer-based information systems in terms of their environmental and organizational contexts. Their primary objective is to cost-justify the solutions. However, they have started increasingly to consider human and organizational aspects as well.[13] Based on these approaches, numerous models have been developed that help in identifying the countermeasures and apportioning the costs.[14] Although these frameworks help in furthering our understanding of IT risks, they tend to impose a 'tidy' structure on to risk assessment. This is because the models are grounded in a merely functional interpretation of organizations.

It is not the intention of this paper to propose a fresh classification of IT risks such that problematic situations could be mapped on to it. In fact the argument of this paper broadens the scope of IT risk management by addressing the issue of the integrity of information systems. It is important to maintain the wholeness of systems because organizations depend so heavily upon information for their success. The availability of information not only helps an organization to co-ordinate and control its internal and external relationships, but also influences the effectiveness of an enterprise. Therefore any disruption in the information and communication systems or in the organizational operations has detrimental effect on the entirety of the concern and the systems that support it.

The use of IT is often related to enhanced productivity and effectiveness of the business, with little consideration given to the integrity issues. Since '. . . information technology has not been in existence, nor has it been stable, for long enough to be well understood; the price of this opportunity is in the introduction of new hazards, implicit in untried systems'.[15] These new hazards always challenge the completeness of an enterprise. There are numerous examples where the use of IT has had disastrous consequences. In the UK we had the recent experience of the

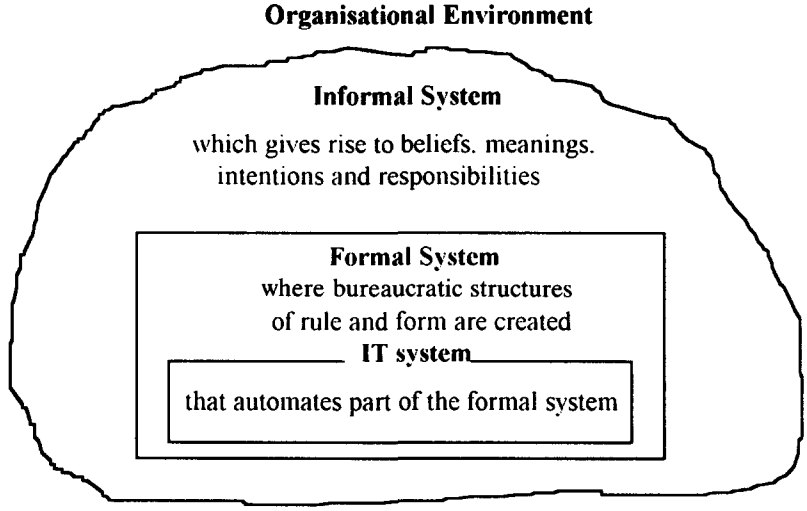



**Figure 1** Nature of the organization (based on Lieubenau and Backhouse, 1990)

Wessex Regional Health Authority's £43 million information system plan fiasco. The system was intended to link together every hospital, general practitioner and district nurse in the authority. The project was a failure and was subsequently abandoned. The reasons attributed to the failure were excessive complexity, imposition of a centralized structure and the resultant uncertain environment.[16] Besides the failure of the system, the organization was also a victim of insider fraud. The result was a complete loss in integrity of the organization.

Only if the integrity of the organizations and systems is maintained is it possible to draw advantages from IT applications, and result in increasing the productivity and efficiency of the enterprise. This has very successfully been demonstrated by the world-famous Royal Marsden Hospital where a patients' record system was installed by Kodak. The Royal Marsden patient administration system was a success because it did not try and do too much over too wide an area at one go.[17] Rather a bottom-up approach was taken where all its options for interconnectability were kept open. Each application was looked at separately and systems were designed which best served the needs of that application. Consequently the system implemented was not overtly complex, was cost justifiable, did not disrupt the existing responsibilities and power relationships, and hence did not breed uncertainty.

In order to maintain the integrity of the organizations, it is important that we have a clearer understanding of the nature of organizations. This would result in not only the successful development and implementation of information systems, but also in minimizing risks associated with IT usage. The emergent belief of most studies is to view organizations as evolving social forms of sense making. Consequently, they allow different groups to relate to each other and the environment. Walsham[18] views this to be a dynamic process of action/context interweaving, which is fundamental to the understanding of the process of organizational change. Consistent with the views held by Dhillon and Backhouse,[19] Land,[20] Liebenau and Backhouse[21] and Klein and Hirschheim,[22] this paper considers organizations to be constituted of informal, formal and technical parts which are in a state of continuous interaction (*Figure 1*).

*continued from page 66*

*Security Management* John Wiley, Chichester, 93–116

[15] ANGELL, I O AND SMITHSON, S (1991) *Information Systems Management* Macmillan, London

[16] KER, N, (1994) 'Small is beautiful' *The Computer Bulletin* **6** (2) 5–6; WATKINS, S (1993) 'MPs push for IT check-up after health scandals' *Computing* (18 February); MILES, R (1993) 'MPs throw book at health chiefs over Wessex fiasco' *Computing* (13 May); (1992) 'MP prescribes NHS IT audit' *Computing* (19 November)

[17] KER, *op cit*, Ref 16

[18] WALSHAM, G (1993) *Interpreting Information Systems in Organisations* John Wiley, Chichester

[19] DHILLON, G AND BACKHOUSE, J (1990) 'Responsibility analysis: a basis for understanding complex managerial situations' in *1994 International System Dynamics Conference* University of Stirling, Scotland

[20] LAND, F F (1992) 'The information systems domain' in GALLIERS, R (ED) *Information Systems Research. Issues, Methods and Practical Guidelines* Blackwell Scientific Publications

[21] LIEBENAU, J AND BACKHOUSE, J (1990) *Understanding Information* Macmillan, London

[22] KLEIN, H K AND HIRSCHHEIM, R (1987) 'Social change and the future of information systems development' in BOLAND, R J, JR AND HIRSCHHEIM, R (EDS) *Critical Issues in Information Systems Research* John Wiley, Chichester

The use of information technology for organizational effectiveness has largely been concerned with the technical part (ie formal administrative and procedural tasks) of an organization. The technical system is supported by, and supports, the formal system of an organization which is characterized by bureaucracy, where concern for rule and form replaces that for meaning and intention. The technical and formal systems exist within a larger informal environment where meanings are established, intentions understood, beliefs, commitments and responsibilities are made, altered and discharged. In any organization, over a period of time a system of fairly cohesive groups with overlapping memberships is created. These social groupings of the informal system have a significant bearing on the wellbeing of an organization. The groups or even individuals may have significant power and may be in a position to influence other informal groups or even the formal structures. Thus when IT is used to manage large organizations, a proper balance is needed between the three sub-systems. Failure to do so generates uncertainty, creates complexity and introduces unnecessary risks.

## Empirical studies

This section presents case studies of two organizations that have experienced the use of information technology. Case 1 is a British National Health Service Hospital Trust where an integrated client information system is being implemented. It represents highly centralized information processing activities. Case 2 is a UK Local Government Borough Council which is characterized by a number of small information systems. The Council is in the process of implementing an organization-wide information and communication network. Findings are based on field work carried out between 1992–1994. Data is drawn from both primary and secondary sources. Primary data was collected from in-depth interviews with users, managers and decision makers in both organizations. Topic guides were prepared for each interview and probing questions used to explore the underlying patterns of behaviour. Secondary sources of data were government reports, internal publications and intra-departmental communications. The case study approach allowed us to mimic the 'real world' thereby facilitating an understanding of the social organization and the relationship with information technology. In this way it was possible to comment on the integrity of systems in place.

### *Case 1: a UK National Health Service Trust*

This case looks into a new system that is being introduced into the 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. The new computer-based information system runs a high risk of abandonment, under-utilization and misuse.

*Purpose of IT infrastructure.* The recent changes in the organization of the NHS prompted by the Griffiths report of 1983 and the more recent Community Care Act (1990), have inspired the NHS Management

Executive and the individual hospital trusts 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 their activities), but also to add value to the health care delivery process. With respect to the recent changes in the health service, 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 was being implemented at this NHS Trust. It incorporates care planning functionality 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. This is facilitated by meeting the demands of the purchasers in providing information to assess the quality and effectiveness of services delivered. Such information is drawn through a process of constant monitoring of care delivery, recording of assessment details and measuring of outcomes.

In implementing the integrated information system, the NHS 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, whether formal or 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 has resulted. 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.

*Semantics of IT infrastructure.* The Trust hospital is characterized by three professional groups: clinicians, nurses and managers. The three groups form their own power structures in the organization. Interviews with members of the these groups revealed conflicting ideologies (ie 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 doctors 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 short-sighted in their approach and only the 'long-stay' wards (which were due to be closed in the very near future) had been sampled for requirements analysis.

*Form of IT infrastructure.* Ideally, the rules specified for the IT infrastructure should adequately represent the real world of the organization.[23] 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, ie 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 and which runs a high risk of under utilization or even complete abandonment.

*Means of achieving the purpose.* 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 (ie between clinicians and managers), the informal organizational norms are very weak, indicating the presence 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, although 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, ie 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.

*Case 2: a UK local government body*

This case illustrates how fairly successful systems can pose a major source of risk if the organizational policy does not match operational procedures. The case material is drawn from a Local Government

[23] CHECKLAND, P B (1981) *Systems Thinking, Systems Practice* John Wiley, Chichester

Borough Council. Unlike Case 1, the Borough Council did not have any integrated computer-based information system but individual departments and sections had their own small information systems. The departments also had their own IT strategies and most information systems were based on 'off-the-shelf' software. This study looks at the systems in one of the biggest departments of the Borough Council, the Public Services & Works Department (PS&W). The Department is further divided into 14 sections with very specialist functions (such as waste management, car parking, civil engineering, transport, etc).

*Purpose of IT infrastructure.* The UK local government is going through a period of significant change. This is affecting the way the services are organized and delivered. The main drivers for the change are the Citizens' Charter and the Audit Commission reports. The changes are becoming visible at two levels. First, there is an increased pressure on various departments and sections to compete with private service providers. Second, the customers are becoming more demanding (especially after the Citizens' Charter[24]). Hence this Borough Council is regarding Customer Care as their top priority.

The central policy office of the Council felt that an IT infrastructure needs to be developed which would facilitate effective communication and better management control. As a result of this, two projects were launched. First was to develop a Geographical Information System, where it was envisaged that a wide area network would be developed. This project however is still at the conceptualization stage. Second was an Information Communication System project where electronic links would be established between all Principal Officers of the Borough Council. It is argued by the members of the policy office that effective 'informal' communication at an inter- and intra-departmental level will inculcate a 'customer culture' in the organization. Hence it will be possible to enhance the level of customer satisfaction. The Principal Officers were expected to report on set parameters such that activities of the decentralized departments and sections could be monitored. It would be some time before a Council wide system is put into place, however the Public Services & Works Department had taken the pioneering role of implementing key features of the new system. This section looks into the consequences of such a move.

*Semantics of IT infrastructure.* The Borough Council is characterized by a highly decentralized IT infrastructure where the work patterns are not technology led. For years the departments and sections have had manual complaint monitoring systems in place. Since the advent of specialist software packages, used by departments and sections, complaint monitoring systems have been built into them. Thus the quality of service provided is regularly monitored at the departmental/section level. For instance, the Waste Management section uses an off-the-shelf package (which runs on Unix) to monitor waste collection in the Borough Council. The computer system, which has been well accepted by the section, helps in penalizing contractors for their wrong doings. Managers of the section see this as customer care at the operational level. The individuals at this level do not see the utility of communication technologies in enhancing customer care, rather they get the feeling of a 'big brother watching them'. Over a period of time the organization has developed potent norm structures, there are fears that these

[24]The Citizens' Charter redefines the contract between the citizen and the state in the UK. It has three underlying assumptions. First, the citizen is entitled to receive some level of service in return for taxpayers' money. Second, the citizen is entitled to know what level of service is being provided. Third, the citizen is entitled to some form of redress if that level is not attained

structures and social groupings would be threatened. Therefore at the departmental/sectional level, where the use of technology has been incidental to the normal functioning of the organization, implementation of any technology-led formal system' faces strong resistance.

The Chief Executives' Office however views the changes differently. In line with the policy of the CEO, it aspires to make the Borough Council a 'networked authority'. The rationale behind this is two-fold. First, it wants to breed a culture of informality (the Chief Executives' office defines *informality* as 'everybody talking to anybody at any time'). It is assumed that this would facilitate effective communication and thereby bring in efficiency in the work practices. This will result in the provision of better customer care although the experiences in Public Services & Works Department are rather different). Second, it visualizes the Borough council as a paper-less office'. The rationale put forward is that every year the Council uses nearly 20 million sheets of plain paper. Since the costs for printing, storing, distributing and disposing paper are enormous, the 'Council is determined to tackle this problem . . . and Electronic Communication is set to provide one of the most effective and exciting solutions'. Thus it becomes clear that there is a lack of consensus on the purpose, form and means of IT usage among different groups. There is a clear mismatch between the Council's policy and the practices at the sectional level which raises integrity questions about the congruity of information systems and organizational practices.

*Form and means of achieving the purpose.* The decentralized nature of IT infrastructure has already been emphasized. Typically two of the sections of the Public Services & Works Department have Unix based systems (ie Waste Management Division and Transport) while others have PC-based systems. In all the Borough Council has 25 local area networks. Since none of the information systems is linked to another, there is no electronic exchange of information among different sections. The need for such exchange is also minimal because their activities have very little overlap. In taking the notion of a customer care culture further, the Public Services & Works Department implemented a small system which draws pertinent information from all sections. Initially this system was manual, but gradually it is being automated. It is envisaged that this will form an integral part of the overall information communication system. Since the activities of all the sections are so diverse, the only commonality found by the manager in charge was the response rate to the complaint calls. These are at present being recorded and processed electronically.

The means of achieving the purpose seems dubious. The top management feels that the customer care objective can be achieved by implementing an information and communication network. Managers at the departmental level (Public Services & Works in particular), in carrying forward the same argument, try to force a technical system onto highly decentralized sections. This is directly in conflict with the existing informal culture which is strong at the section level. There is a general feeling among individuals at the operational level that the whole exercise is futile. They regard the new system as nothing more than an electronic letter ledger. A manager of the Waste Management section confirmed this by saying that at the operational level one sees real customer orientation and 'and what they (the Chief Executives' Office) are doing is not customer care'. Thus in trying to impose technical

Table 1 *Summary of findings*

| | UK NHS example | UK local government example |
|---|---|---|
| Purpose of IT infrastructure | To add value to the health care delivery process | To increase the level of customer satisfaction |
| Semantics of IT infrastructure | The IT infrastructure is interpreted differently by the various stakeholders | There is no common consensus in the purpose, form and means of IT infrastructure |
| Form of IT infrastructure | An integrated system where rules and procedures do not represent the 'real world' | Excellent decentralized small systems but an inconsistent and an incoherent communication system |
| Means of achieving the purpose | By introducing a computer-based information system and expecting formal and informal work practices to adjust accordingly | By introducing communication technologies to monitor and control highly decentralized departments |

controls onto a predominantly informal setting, the integrity of the organization and the formal systems in place is being sacrificed. Such a situation could not only result in a loss of productivity but also a lower standard in customer care.

## Summary of findings

The research carried out gives an opportunity to examine the relationship between the use of IT, the integrity of the information systems and the associated risks. *Table 1* summarizes the findings. It becomes apparent from *Table 1* that even though the nature and scope of IT infrastructure in the two cases is significantly different, they experience similar problems of system integrity. In Case 1, integrity of the organization is in question because a flawed technical system is being implemented and is forcing a new formal structure onto the existing work practices. In Case 2, the problem is of implementing a centralized technical control system on a largely decentralized organizational structure.

The findings support the theoretical notion that although information technology is considered to be a means of enhancing the efficiency and effectiveness of an organization, in practice an inconsistent use is counter-productive.[25] The two case studies clearly illustrate the implications for the integrity of systems when the use of IT is restricted just to the technical components (ie formalizable processes) of the organization. They also show that when computer-based systems are imposed onto the informal environments the integrity and wholeness of information systems is affected. As a result, organizations run the risk of system under utilization, non-achievable system objectives, or even complete system abandonment.

To minimize risks, managers in organizations will have to devise appropriate ways of coping with the use of IT and hence maintain integrity of the enterprise. While there is no universal 'recipe' for minimizing risks, IT professionals will have to evaluate the nature of the organizational environment before considering whether and how to

[25] BRYNJOLFSSON, E (1993) 'The productivity paradox of information technology' *Communications of the ACM* **36** (12) 67–77; WEILL, P (1993) 'The role and value of information technology infrastructure: some empirical observations' in BANKER, R D, KAUFFMAN, R J AND MAHMOOD, M A (EDS) *Strategic Information Technology Management: Perspectives on Organisational Growth and Competitive Advantage* Idea Group Publishing, Middleton, PA

implement any IT based solutions. They will have to address issues arising at three levels: technical, formal and informal. At a technical level the choice of an appropriate technology and design methodology is very important. The use of a hard approach, such as SSADM, limits the consideration of the 'real world' issues. This is especially the case when the problem situation is characterized by conflicting objectives (for example the NHS Hospital Trust case). Equally important is choice of hardware and software which would allow 'interconnectability' and 'media independence'.

At a formal level an organization needs structures which support the technical infrastructure. Therefore formal rules and procedures need to be established which support the IT systems. This would prevent the misinterpretation of data and misapplication of rules in an organization and help in allocating specific responsibilities. If a new technology is being implemented, there is a need for a formal team which gives strategic direction to the project. Finally, a clearer understanding of the structures of responsibility, existing and new, formal and informal, needs to be developed. This would facilitate the attribution of blame, responsibility, accountability and authority.[26]

The informal level needs to address more pragmatic concerns. It is often the case that a new IT infrastructure is presented to the users in a form that is beyond their comprehension, causing problems of acceptance. Users should be made aware of all the features and this should be supplemented by an ongoing education and training programme. The emphasis should be to build an organizational sub-culture where it is possible to understand the intentions of the management. An environment should also be created which is conducive to the development of a common belief system. This would make members of an organization committed to their activities. All this is possible by adopting good management practices sensitive to formal and informal dimensions of the organization. Such practices have special relevance in organizations which are highly decentralized and thus have an increased reliance on third parties for infrastructural support (for example the UK local government case).

## Conclusion

The paper supports the argument that by maintaining the integrity and wholeness of information systems, the risks associated with the use of IT can be minimized. Although the discussion in the paper is based on the key findings of the two case studies, it may be generalized to any organization that is experiencing change due to the use of IT. The three concerns identified in this paper (ie technical, formal and pragmatic) form the basis for developing an information system which can maintain, rather than threaten, organizational integrity. By considering the more pragmatic issues, it is possible to capture the organizational structures in their cultural contexts. This helps the system developer to understand the object system better, thereby securing the integrity of the new IT infrastructure.

[26]BACKHOUSE, J AND DHILLON, G (1993) 'A conceptual framework for secure information systems' in *The Tenth World Conference on Computer Security, Audit and Control, COMPSEC* Elsevier Advanced Technology, London