AN EVALUATION ON INFORMATION MANAGEMENT: A CASE STUDY OF A NATIONAL PUBLIC ORGANIZATION

Suhaidi Hassan *PhD*[1], Juliana Aida Abu Bakar[2], Mohd Hasbullah Omar[2], Hatim Mohamed Tahir[1], and Mohamad Amir Abu Seman[1]

[1]Department of Computer Science, Faculty of Information Technology
[2]Department of Management of Technology, Faculty of Management of Technology
Universiti Utara Malaysia, 06010 UUM Sintok, Kedah.

Abstract

As the business environment nowadays faces stiff competition and as information and communication technology increase in sophistication and complexity, organizations are facing even more challenges and difficulties in managing information. Therefore, it is vital for organizations to evaluate their information management on regular basis in order to gain competitive advantages. This paper presents an overview of an evaluation on information management involving information storage, information processing, and information retrieval in a national public organization. The primary data was collected by means of field visits, series of observation and semi-structured interviews with key personnel of the organization. This paper also discusses on complications encountered when having different systems with different platforms, information security considerations when dealing with ISs and technologies outsourcing projects, and consequences of having very dependent on outside vendors. It further suggests several recommendations to improve the information management of such organization.

Keywords: Information management, IT/IS outsourcing, Public organization

1.0 INTRODUCTION

Information technology (IT) and information system (IS) are major factors in shaping the organizational business processes to gain competitive advantages. Recent advances of IT are bringing significant changes to organizations unanticipated even a few years ago. Here, the term IT is defined in a broad sense as "technologies dedicated to information storage, processing, and retrieval." The notion of IS focuses on hardware, software, networks, procedures and policies, and personnel (Turban, Mclean, & Wetherbe, 2004).

This study is carried out to evaluate the information management of a national public organization and to suggest appropriate recommendations for improving the information management. The evaluation however is limited to business processes involving information storage, processing, and retrieval. This paper discusses the issues and challenges in managing information and further suggests appropriate recommendations to improve the information management of such organization.

1.1 Information Management: Key Issues

It has been a decade since IT and IS has played an influential role in organizations. The effective use of IT and IS in managing organizational information has been associated with several key issues. These key issues, as listed in Table 1, have been identified from the literature (Yang, 1996) according to their relevancy to the selected organization.

Table 1: Several key issues in information management in public organization

Key issues	Explanation
Data security	Protecting software and hardware to prevent information from being changed, destroyed or stolen by illegal users.
Data resources	Managing business data resources so that they can be accessed and utilized appropriately.
Integration of IT	Integrating data processing, telecommunications, office automation, multimedia and other technologies.
Database management systems	Using database management systems to manage a large amount of data in business.
Recruiting, training and career development of IS personnel	Recruiting, training appropriate IS personnel, and providing them adequate career development and promotion path.
Regulations of software/hardware procurement and system outsourcing	Defining reasonable software/hardware procurement and system outsourcing regulations to eliminate tedious or unreasonable limitations.
Measuring and improving IS productivity	Measuring existing IS performance, improving or updating obsolete systems.

These key issues however differ in ranking from one country to another. In the United States (U.S.) for example, integration of IT ranked in the first place but in Taiwan, it ranked fifth. Other key issues such as data security, data resources, database management systems, and recruiting, training and career development of IS personnel ranked third, fourth, fifth, and eighth respectively in Taiwan but ranked fifth, fourteenth, ninth, and seventeenth in the U.S. (Yang, 1996). There is however very limited evidence of such rankings in Malaysia.

IT and IS evaluation has long been considered a difficult and elusive domain. Many reasons have been offered to explain the difficulties in evaluating IS investments. A summary of common difficulties are as shown in Table 2 (Giaglis, 1999):

Table 2: Common difficulties in evaluating IS investments

Factors	Reasons
Cost-Related	• Estimating the cost and time to develop new applications is difficult and unreliable. • Human and organizational costs are often neglected during evaluation.
Benefit-Related	• IS benefits may include intangible, indirect, or strategic advantages that are inherently difficult to express in quantitative (especially monetary) terms. • IS benefits are indirect to business and therefore indistinguishable from other confounding factors (for example, people, processes, and strategy). • Many applications are targeted at achieving second-order effects that are difficult to predict and measure.

	• Fractional IS savings cannot be aggregated to provide realistic savings on an organization-wide scale. • The planning horizon (for which benefits must be assessed) may be longer than the forecasting horizon (for which benefits can be assessed). • Organizations may simply be unaware of the potential benefits of innovative new systems.
Risk-Related	• The life span of IS is uncertain (due to technological obsolescence and changing requirements). • IS impacts depend on a number of external factors that may lie outside the sphere of organizational control.
Methodology-Related	• Financial and accounting techniques may be inappropriate for assessing IS investments. • Usually IS is part of a wider business reorganization and hence IS investments cannot be evaluated out of the context of the overall changes. • Tasks left out of the IS scope must also be evaluated as they can contribute significantly to overall costs.
Political	• Project champions tend to underestimate costs and overestimate benefits.

Besides considering the effect of the investments towards the monetary side, the organization would also have to consider the business processes involved in the evaluation process. In view of the recent focus of much IS research on the issues of business processes change and business engineering, it seems surprising that only a limited number of researchers addressed IS evaluation at the level of the business processes. These researchers include:

i. Ginzberg (1979) who, 25 years ago, wrote: "*Changes to processes are the link between changes to information and organizational outcomes. It is only once we understand how the new system will be used that its value can be estimated. Thus, efforts to quantify benefits should focus on the changes in organizational processes that will result from changes to IS.*"

ii. Farbey et al. (1992) argued for the need to abandon the IS project as the fundamental unit of analysis in IS evaluation and adopt the wider concept of the business process instead. In particular, the authors asserted that "*when the IS is part of a wide ranging set of changes ... it is almost impossible to determine the proportion of any benefit which can be said to stem from any component of the change. It is only possible to evaluate the costs and benefits of the whole package of changes.*"

iii. Farbey et al. (1993), reported that "*...a major change we have detected is that the big questions are to do with the value added by transformations in which IS/IT plays, maybe, a crucial role, rather than about putting value on to the IS/IT contribution. The traditional unit of evaluation was the application. In the future ought we to take a more holistic view in considering the change in all its parts?*"

It is found that in evaluating the IT and systems, considerations for business processes involved have to be made. Hence, this research looks into three areas of information management that involve business processes, which are information processing, information storage and information retrieval.

1.2 Nature of Selected Organization

The selected organization is one of the national public organizations that closely related to national interests. This selection is made upon our belief that such organization will have a proper information management because of its nature. With proper information management, it is estimated that the process of evaluation will run as thorough as possible across organization.

This paper presents an overview of an evaluation on information management of that organization. The organization heavily depends on the efficiency of the information flow in dealing with its daily operations and business processes. The name of this organization is however undisclosed to avoid unforeseen circumstances.

2.0 EVALUATION METHODOLOGY

This study utilizes field visits, semi-structured interviews and random observation approaches. It focuses on the evaluation of the core business processes that involve information management by that organization to carry out their day-to-day operation by the management and staff. During the field visits, the researchers made random observations and held a series of discussions with the personnel involved in the daily operations of the organization. These include meetings with the directors and staff of the divisions within the organization. All information gathered is according to the scope of this research. The collected information is then analyzed to meet the following:

- To identify the business processes involved in the day-to-day administration of the organization;
- To chart the workflow of each process and identify the redundancies or bottlenecks of their operations; and
- To provide cost saving recommendations in improving the efficiency of the operational process.

The outcomes of this study are dedicated recommendations for improving the information management of the organization, an outline of potential risks that the organization might experience in future, and other applications that the organization might deploy to improve its services to the public.

3.0 DISCUSSIONS

The organization has to complete enormous tasks and overcome challenges to reach its objectives in this era of globalization and borderless world. The most challenging one is that how the organization and its representatives throughout the nation will consolidate

and manage its vast distributed resources. In subsequent sections, the issues and challenges that the organization has to face especially in coordinating and managing its IT resources are discussed.

3.1 Conglomerate of vendors

In implementing IT outsourcing, the organization has appointed several vendors to serve different element of the IS, namely hardware, network infrastructure, and systems development. Thus, it is observed that several different companies have controls to different but interrelated components of the organization's IS. This eventually makes the management of IS more complex. It creates a number of problems to the organization in delivering the business services to clients. It also adds the difficulty level for the system administrator in maintaining the system. Several problems caused by the conglomerate of vendors have been identified and discussed.

3.1.1 Vague Point of Reference

When several different systems are interrelated to each other, there is noticeably a problem of chain of commitment in the overall system. If there are several vendors that take a responsibility for several different systems, then we will have several points of references, which make it difficult for the system administrator to maintain the systems.

Since the information management is being catered by several different vendors, there exist difficulties in coordination and responsibility. If problems exist in one of the systems, most vendors will start pointing fingers to one another and awkwardly try to ignore the problem. These problems exist because there is no clear policy on the point of reference.

3.1.2 Increase Duration of Downtime

The point of reference problem has caused difficulties for system administrators to troubleshoot the actual problem. The longer the troubleshooting process, the more time is needed to actually fix the problem. Sometimes, more time is also needed to figure out which vendor is responsible for handling certain problem rather than the time needed to fix the problem.

Even when the problem is fixed, they must ensure that the alteration on the system does not give any impact on other related systems. If there is so, the respective vendor needs to be notified about the alteration. They have to ensure that the data can smoothly flow from one system to another. And when it comes to commitments from several parties a on certain problem, then more time is needed for the communication and the process of transferring the commitments to their systems.

3.1.3 Chain of Commitment

When several vendors controlled several components of the system, a chain of commitment situation occurs. In this situation, one party has to depend on the other party to complete their job in delivering the product to the customers. Consider this analogy; for a tire manufacturer to make quality tires for the market, they have to depend on the rubber suppliers to supply the best raw materials to them. If the suppliers provide a low quality rubber, then the manufacturer will produce low quality tires.

In the case of this organization, different departments use different types of systems that are interdependent. Ideally, these different systems should be able to serve each other. Unfortunately, these systems are developed by different vendors whereby different development technologies are used in terms of their operating systems and databases. When there is a need for modification in one system, other systems has to ensure that it can accept data from the modified system. If the modification does not change the format or type of the data, then there should be no problem. Nevertheless, when the modification changes the format of the data, then other systems need to be modified accordingly to receive the new format.

3.2 Obsolete Technologies

Most computer systems in this organization were acquired for approximately seven years ago. The processing speed, operating systems, and memory sizes of these systems are insufficient to serve an increasing amount of data and business transactions. The increasing amount of data should be properly handled by acquiring more powerful processors and larger memory sizes to avoid any disruptions during data processing. Thus, IT resources must often be reviewed because they can be considered obsolete after five years of acquisition.

The lack of IT reviewing process will affect the scalability of IS and the performance of such systems in the long run. This will delay the data processing and eventually the whole system operations and information flow. The subsequent section will further address these issues.

3.2.1 Scalability

Scalability refers to the ability of a computer, product, or system (hardware or software) to continue to function well as it (or its context) is changed in size or volume in order to meet a user need (Laudon & Laudon, 2002). It is related to the maintainability of the technology to keep operating over time and the possibility to significantly increase or decrease capacity without making disruption.

In order to store a large amount of data, the IS at this organization use databases with a client/server architecture. In a client/server network, end-user personal computers (PC) or clients are interconnected by local area networks and share application processing with network servers, which also manage the networks. Servers should be able to handle a high traffic of data and avoid network congestion during peak hours. However, it is found that servers at one particular branch hardly met this requirement. The PC clients for

certifying specific documents have to wait approximately a minute to get access to databases. If a PC client performs one minute per data access, the process to get documents being certified per se will take more than five minutes. Imagine if there are 30 documents to be certified, it took them approximately two hours and 30 minutes to clear the process!

3.2.2 System Performance

The overflow of data can be hazardous to system performance because it may slow down the processing time, or even halt the system from functioning. The system performance should always be in tip-top condition especially when dealing with highly confidential data. As data is kept in several databases, it is important to acquire a powerful server or multiple servers to ensure a smooth flow of data.

It is found that the organization has two different databases from different vendors. The fact is that these databases could not read to one another and are functioning as two different entities. It is somehow very unfortunate because the officers will have to perform data entry twice in both databases. This can lead to unintended mistakes when the same data is being keyed into different systems. This repetitive work will also consume time and energy that can supposedly be channeled to other working activities.

3.3 Brain Drain

Employees who involve in managing and maintaining IS of most national public organizations are originally recruited and appointed by the Public Service Department of Malaysia (PSD). The staff is transferable to any other government agencies as directed by the PSD. This policy eventually affects this particular organization by putting it into a situation known as *brain drain*. Problems that are associated with this brain drain situation are as follows.

3.3.1 Lack of Experience

Newly reported employees need to be familiar with the systems running in the organization. This consumes time and cost for staff training. However, the process of gaining the experience in using the systems and handling the problems involving the systems is much more time consuming. This eventually results in denial-of-service situation if anything happens to one of the systems.

3.3.2 Quality of Services

The effects of brain drain would be serious due to the quest of our nations towards globalizations. The organization needs to improve its services as well as the systems' responses and rate of service per person in order to accommodate the ever increasing public demands. Therefore, the systems cannot afford to have even a single glitch in everyday transactions.

3.3.3 Fraud

In this era of globalization, frauds are done much easier although the organization feels that its systems are well protected. The effect of brain drain would provide golden opportunity for fraudsters to make bogus documents based on the experience gained by the former staffs (who are transferred) since they know inner workings of the systems in the organization. This would result in a security threat to the nation.

3.3.4 System Control

The organization should take proper steps to improve their brain drain cause and effect since the staff is transferable to other Government agencies. Instead of giving training to new staff on the operations of the existing systems, it should consider on upgrading the systems on its own. This would eventually give the organization full control of its own systems since the systems are modified and maintained by its staff. Though the organization outsourced systems development to vendors, the staff can eventually know the insides of the organization's systems and hence the dependency on vendors can be minimized.

3.3.5 Acquiring New Knowledge

In order to keep up with the advancement of new technology, the organization needs to be more competitive to the outside threat concerning its computer systems. The government is actively considering Open Source systems where the system can be personalized according to the needs of the specific organization. This will enhance the security since the system can only be understood by the developers of that system. The brain drain however will slow the process of moving towards Open Source systems because the staff in charge is likely to be transferring in and out.

In summary, brain drain would impart severe effects, both short and long terms to the organization. Should this situation cannot be avoided, such organization must take proper consideration and action to minimize these effects.

3.4 Information Security

Since this organization have many branches throughout the country and foreign offices, transferring or sending of data across the network has to be done in an extremely careful manner. It has come to our understanding that all information networking among all branches throughout Malaysia and other foreign countries are provided by networking vendors. Although the transmissions of data are encrypted, information security can never be compromised because encrypted data can always be tapped anywhere in the distributed environment. Several inquiries should be considered such as the following:

- Can the network vendors be trusted?
- Has the network vendor staff undergone security screening process?
- Can the provided network be trusted?

- What if the network is tapped or eavesdropped at certain location? Does the organization able to monitor this situation?
- Is there a possibility that the data are being stolen and manipulated without knowledge?

The information security consideration has been the top priority in implementing any IT and IS projects in foreign countries (Khalfan, 2004). It is therefore vital for such organization to take precautions since lack of information security will eventually bring threats to the nation.

3.5 Disaster Recovery

It is found that the organization has assigned their disaster recovery to the third parties. Before this, it took several days to recover from a disaster. These disaster incidents really disturbed the normal business processes of the organization. Due to a high risk interruption, a test run has been done to their disaster recovery plan. According to them, it takes only few hours to totally recover from certain types of disasters. However, the organization has to rely on the third parties to keep or archive their business records and managing the disaster recovery center continually for 24 hours a day because of the high cost of such infrastructure. This will eventually lead to issues on information security as discussed in the previous section.

3.6 Procedures and Policies

The organization has established a specific division to cater IS of the organization. This division has written some documentations pertaining to procedures and policies (PP). These documentations generally adapted guidelines provided by the Malaysian Administrative Modernization and Management Planning Unit (MAMPU). However, it is observed that there is still lacking of PP that covers the following issues.

3.6.1 Electronic Data Processing and Communications

The data transmission between branches is done throughout a large and distributed network. This means that it is vulnerable and exposed to data tampering at various locations anywhere and anytime. Moreover, the processes of data encryption and authentication are handled entirely by third parties.

3.6.2 Security Policy for Information Systems

A security policy of IS is vital to uphold the integrity of such organization. It is found that such policy should be bounded by MAMPU security policy guidelines. According to the respective division, they have tried their very best to follow that guidelines. However, it is observed that there are still rooms for improvement in their implementation.

In short, the issues of conglomerate of vendors, obsolete technologies, brain drain, information security, disaster recovery, and procedures and policies are among few of the

issues that we have managed to obtain. Nevertheless, we are confidence that the organization have also raised and tried their best to resolve some of the issues stated.

4.0 RECOMMENDATIONS

Based on the findings as discusses in the previous section, several recommendations are put forward for the organization to take into considerations.

4.1 Information Systems Acquisition and Technology Review

As far as the organization is concerned, strategic IS should be secure from potential threats and hazards, scalable as business activities expand, and more beneficial against cost to the organization. The recommendations for IS, especially software, therefore as follow:

- Staff should indulge in the development stage of strategic IS even though the systems are outsourced to several vendors. This will automatically train a member of staff with inside expertise of such systems and can further save time and monetary costs of after sales services. Eventually, this expert can help organization impose defense strategies to get control of the systems by protecting them from potential computer crimes and criminals.
- It is crucial to review IS often as business activities expand to make sure they can handle increasing numbers of transactions and users while maintaining a high level of performance and availability.
- The external acquisition of software should consider on user acceptance, favorable cost-benefit ratio, low maintenance, scalability, ability to integrate with other systems, minimal negative cross-impacts, and reusability (Turban, Mclean, & Wetherbe, 2004).

By implementing the recommendations above, issues regarding software as mentioned can hopefully be resolved. However, many successful stories of IT implementation in an organization suggest that in order to achieve competitive advantages of IT, the organization has to rely heavily on full commitment from the top management and IS specialists, and have a strong relationship and understanding between them.

4.2 Knowledge Management

People is one of the IS components that plays a major role. The two groups of people are end-users or also known as clients who use an IS or the information it produces, and IS specialists who develop and operate IS (O'Brien, 2003).

A knowledge management system is one of the solutions for reducing the effects of brain drain when personnel leave the department to other government agencies or private organizations. The system dictates all the problems and experience the personnel gain from the work they done at the department in dealing with the existing IS. It can be a one-stop resource for the new personnel to look at or other colleagues to share their

experience in dealing with the problem known in handling the department system in their daily operations. The use of a knowledge management system will also reduce the cost for training new personnel.

IS specialists need to be recruited by the organization itself to control, service, and maintain the existing systems. The role of the IS Specialists should also be broadened to create, develop and apply future systems or application required. If the need to outsource projects arises, the personnel should involve in the development actively to ensure that the dependant on vendor would be minimized. Since outsourcing is an increasingly sensible option since the organization does not have the necessary time or skill to accomplish, it is important to properly manage the outsourced work and vendors. Vendor relationships must not be transactional and contractual only, but also strategic and joint (Turban, Mclean, & Wetherbe, 2004).

4.3 Data and Information Resources Security

In an organization, data and information are stored in databases or flown around the IS. One of the methods to ensure the data is safe is through data encryption (or cryptography). Data encryption is a way of transforming any information or data to unreadable format for security reason. There are, however, several key issues that need to be considered when implementing such method:

- The cryptography system must be based on the requirement and the operating environment of the organization.
- The cryptography key should be well-managed.
- The cryptography disaster recovery plan must be available and efficient.
- Hardware/equipment should be secured as well.

In addition to the data/information security using cryptography, it is also important to have a closer look at the security of the equipment and hardware used in operating the information. If the equipment is vulnerable to any threat, it means that the information is also vulnerable. It is observed that the equipment in the organization is serviced by a vendor by leasing elsewhere. Permitting the vendor staff working with the equipment would expose confidential data and information to a distrusted party, which indirectly jeopardize our nation security.

Therefore, it is recommended that the organization has its own technical staffs operating and servicing all the equipment. By having these technical staffs, the critical and confidential data and information of such organization can be preserved from intentional threats outside the organization.

4.4 Documentation on Procedures and Policies

From the earlier section, it is found that the exposure of critical information to the many parties may jeopardize the security and confidentiality of the information. We

recommend that the organization follow the guidelines provided by MAMPU security guidelines (MAMPU, 2002) in terms of securing the flow of information:

- To ensure the information flow in and out of the organization is totally safe by employing security measures such as cryptograph.
- To appoint or train IT personnel to be an information security officer.
- To have written policies on all aspects of computer, network and information security.
- To have personnel trained to be on alert of any security breaches that may occur when transmitting or receiving data.
- To have policies in terms of information handling who can handle what kind of information. This should also specify what vendor can and cannot do while attending any IT related trouble-shooting.
- Sensitive areas such as server rooms should be well-guarded. This can be done by having written policies and biometric-kind of entrant to sensitive servers.

As far as the disaster recovery is concerned, the organization should also have a contingency plan should the need arise. By relying on third party disaster recovery, the organization is putting their fate on just the third party. It is recommended that the organization has its own disaster recovery center or shares it with other government institutions. It is acknowledged that the cost of setting-up the disaster recovery center and maintaining it might be high, but the cost can be distributed among various government institutions that share the disaster recover center.

5.0 CONCLUSION

In any organization, there are bound to be loopholes in IS being developed. It is the role of an organization to minimize the loopholes by getting feedback from users, customers, and perhaps, independent third party evaluators. This process must be done to ensure that the organization's IS are safe and secure. An organization should always be well-prepared for any undesired situation. Similarly with this in mind, it is certainly believed that this respective organization will take necessary action upon abovementioned recommendations to avoid untoward incidents. Although these recommendations might not be extensive, it can at least be guidelines for such organization to follow.

ACKNOWLEDGEMENT

We would like to extend our gratitude to Universiti Utara Malaysia for the research grant and the top management and IT staff of the organization for their commitment and support.

REFERENCES

Farbey, B., Land, F., & Targett, D. (1992). Evaluating Investments in IT. *Journal of Information Technology*, 7(2), 109-122.

Farbey, B., Land, F., & Targett, D. (1993). *How to Assess your IT Investment: A Study of Methods and Practice*. Oxford: Butterworth-Heinmann.

Giaglis, G. M. (1999). On the Integrated Design and Evaluation of Business Process and ISs. *Communications of the Association for ISs, 1*(19).

Ginzberg, M. J. (1979). Improving MIS Project Selection. *Omega, 7*(6), 527-537.

Khalfan, A.M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive study of two sectors. *International Journal of Information Management, 24*, 29-42.

Laudon, K.C., & Laudon, J.P. (2002). *Management ISs: Managing the Digital Firm* (7th ed.). New Jersey: Prentice Hall.

MAMPU (2002). *Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS)* (2nd ed.). Putrajaya: Malaysian Administrative Modernization and Management Planning Unit.

O'Brien, J.A. (2003). *Introduction to ISs: Essentials for the e-Business Enterprise* (11th ed.). New York: McGraw Hill Irwin.

Turban, E., Mclean, E., & Wetherbe, J. (2004). *Information Technology for Management: Transforming Business in the Digital Economy* (4th ed.). New York: Wiley & Sons.

Yang, H. (1996). Key information management issues in Taiwan and the US. *Information & Management, 30*, 251-267.