DATA LEAKAGE IN ICT OUTSOURCING: RISKS AND COUNTERMEASURES

Yap May Lin[1], Mas Idayu Zakariah and Azlinah Mohamed[2]

Faculty of Computer & Mathematical Sciences
Universiti Teknologi MARA

maylin@tmsk.uitm.edu.my[1]
azlinah@tmsk.uitm.edu.my[2]

ABSTRACT

Having been among the top ranks of worldwide ICT outsourcing indices for a number of years, Malaysia is familiar with the role outsourcing has played in changing today's business landscape. However, concerns of data privacy and security, and the risks of data leakage arise during the course of outsourcing as the process may involve the exposure or handling of sensitive and confidential client and organization information to outsource providers since the company has little control over its outsourced data when it is in the provider's possession. Empirical findings on the risks and countermeasures of data leakage are presented, in the context of outsourcing in Malaysia. From the findings, it was apparent that the inherent risks were significant and that the countermeasures were positively correlated to reducing the risks. This study contributes to the limited pool of knowledge on data leakage issues in outsourcing. Organizations engaging in or contemplating outsourcing will find the results beneficial not only in understanding the data leakage concerns but also in supporting the high priority for these concerns to be addressed. However, more effort is required to enforce the countermeasures as prudent precautionary routines to reduce data leakage risks.

Keywords: ICT Outsourcing, Data Leakage, Risks, Countermeasures.

INTRODUCTION

Malaysia's outsourcing sector is predicted to increase by at least 20% in 2010 from about US$1.1billion in revenue in 2009. This was reported by Pikom's Outsourcing Malaysia in Bernama.com (2010, February 4). Malaysia was ranked as the third most ideal information and communication technology

(ICT) outsourcing destination according to AT Kearney Inc.'s 2009 Global Service Location Index and was ranked among the top five most preferred locations in the world for ICT-shared services and outsourcing by Frost & Sullivan Inc.'s 2007 Global Shared Services and Outsourcing Hub (Lee, 2009; *www.outsourcingmalaysia.org.my*). Malaysia is thus quite familiar with the field of outsourcing and the role it has played in changing today's business landscape. With many businesses concentrating on core competencies, non-core business activities, such as network operations, data centre, helpdesk, and disaster recovery, are being outsourced to specialized service providers (Beulen, Ribbers & Roos, 2006).

Organizations that outsource their ICT functions contract agreements that require the transfer of full or partial responsibility for delivery of ICT services to their providers. Thus, the provider may take possession of some or all of the property and staff of the organization's IT department. In doing so, organizations may fail to give due diligence to the risks involved when outsourcing a selection or all of its ICT functions, in particular, data leakage risks when sensitive and confidential client and organization information are exposed or handled by outsource providers. Although close monitoring may be helpful in reducing data leakage within the organization, the organization becomes vulnerable when interacting with external entities (service providers) during outsourcing. Some common ways client data may be at risk include the careless or deliberate misuse of IT, staff misconduct and illegal acts, involvement of unscrupulous or careless service providers, and incorrect handling and disposal of confidential data. According to a 2005 Bernama report, very few local companies in non-financial services sector practice any data destruction procedures. The financial services industry dictates the strictest compliance to proper data management. However, only an estimated 70% of local companies in the financial services sector follow proper data disposal processes (Bernama, 2005, July 13).

With the growing number of sophisticated hacking and cyber threats, the threat of a security breach through outsourcing takes on an ominous note. Such was the case of the IT staff who worked at an overseas outsourcing company in Pakistan. She had obtained sensitive patient documents from the University of California, San Francisco, Medical Centre (UCSM) through a medical transcription subcontractor that she worked for (Collett, 2004). She threatened to post the patients' documents online unless UCSM paid wages owed to her by the US-based company that had outsourced the work to Pakistan. Suffice to say that the amount was paid and she kept her promise. And then there was the case of CardSystems Solutions that was hit by hacker attacks in 2005, potentially exposing 40 million credit card numbers of various brands to online intruders. Visa, Mastercard, and American Express contracted CardSystems with the provision of processing credit card transactions for small-medium businesses. The company failed to meet contractual requirements as it had violated their security rules by the improper storage of credit card data (Weiss, 2005).

Post literature featured substantially on the overall ICT outsourcing risks (Arshad, Yap & Mohamed 2007; Dhar & Balakrishnan, 2006; Tafti, 2005; Gonzalez, Gasco & Llopis, 2005) but there seemed to be only a limited number of research studies conducted specifically on data leakage (Karyda Mitou & Quirchmay 2006; Klosek, 2005; Khalfan, 2004). One to the latter, some of the countermeasures adopted in this study were derived from available practitioners' resources. Clearly, the gap with which this study seeks to address lie in the current situation of data leakage risks faced and the countermeasures adopted by practitioners. The objective of this paper is to present empirical findings on the risks and countermeasures of ICT outsourcing data leakage among some Malaysian organizations. The findings have a twofold contribution. To researchers in this discipline, the findings add to the existing knowledge base and address the gap using local data. While, to organizations that practice outsourcing or intend to outsource, the information from this paper will provide a clearer insight on the data leakage concerns that must be anticipated and thus addressed with precautionary measures.

DATA LEAKAGE IN ICT OUTSOURCING

The issue of data leakage arises when business organizations collaborate in order to gain access to knowledge and expertise that they are unable to develop on their own for various reasons. By contracting or outsourcing with other organizations (service providers) to execute various activities, these (client) organizations were able to concentrate their activities in their core competencies and yet enjoy the benefits of strategic alliances with their collaborators in terms of increasing flexibility of IT services and economies of scale (Turban et al., 2009; Beulen et al., 2006). However, during the course of outsourcing, data leakage of a client organization's information asset can occur due to acts of accidental or intentional disclosure by the outsource provider. For instance, the client's data that is kept in the service provider's storage medium is lost when the storage medium is not securely protected, when the hardware itself that contains the data is lost or stolen, the service provider exposes and sells the information asset to the client's competitor, misuses the data for purposes other than the outsourcing activity, and uses the information asset to threaten the client (Vijayan, 2006; Weiss, 2005; Collett, 2004). One of the key findings in a study conducted by Khalfan (2004) indicated that security issues (data confidentiality) is the most prominent risk factor of IT outsourcing in a Kuwaiti environment. With the occurrences of problems such as security breaches, error-prone software development, and many service quality complaints, it is not unexpected that according to the Global IT Outsourcing Study 2004, published by DiamondCluster International, client companies are increasingly dissatisfied with providers (Bakalov & Nanji, 2005; Weakland, 2004). As a provider not only delivers ICT services but has to undertake responsibility for executing specific business processes for the client, providers must have in-depth knowledge of the specific business processes involved (Turban, King & Lang, 2009; Beulen et al., 2006). This acquired knowledge coupled with a pattern of work where providers act for several client organizations, simultaneously and consecutively, provides ample opportunities to either accidentally or intentionally leak information to competitors and to betray the organizations hiring their services if they choose to do so (Hoecht & Trott, 2006). This particular outsourcing risk of data leakage that centres on sensitive knowledge and technology has been mentioned in past literature on ICT outsourcing but has not been adequately addressed.

Outsourcing entails a considerable degree of "openness" and hence, carries a high exposure to the data leakage risk of losing commercially sensitive knowledge to competitors. It is a process that involves dealing with sensitive client information that may expose a client company to liability. And, in the event of a security breach or attack, not only will the organization's security and confidentiality be compromised, the business recovery planning will be difficult to initiate (Lee, 1996; Scott, 1996). In addition, although providers claim that they are trained in up-to-date technologies and are aware of the latest data security measures, the difficulty lies in client organizations being able to establish such claimed expertise and knowledge (Karyda et al., 2006). Past literature has invariably cited data security concerns as a risk factor in outsourcing (Arshad et al., 2007; Beulen et al., 2006; Hoecht and Trott, 2006; Gonzalez et al., 2005; Klosek, 2005; Khalfan, 2004). When the IT function is provided in-house, the security of the data is under the organization's control. However when ICT is outsourced, the organization can no longer retain full control of data security. Thus, it is important for organizations contemplating to outsource their ICT functions to give serious considerations to preserving the security and privacy/confidentiality of their information assets (Karyda et al., 2006; Beulen et al., 2006; Musaji, 2005; Tafti, 2005).

Data security is an integral part of all outsourcing activities, and it is important for the client organization to reach an agreement with the provider with regards to the type and level of data security needed in relation to the outsourced activities. Most outsourcing contracts have stringent and tightly defined service-level agreements (SLAs) with incentives and penalties that aim to make the outsource provider deliver better service to the end users.

However, rather than relying on SLAs to sue the provider for damages when problems occur, it is preferable to ensure that preventive measures are taken to reduce the level of risk involved. Consequently, it is important that client companies continuously monitor that their providers comply with data security and confidentiality requirements in the proper handling of data access, usage, storage, sharing, and transmission. This consideration for the security of outsourcing arrangements should be practiced at the beginning of the contractual agreement, during the execution of the outsourcing and finally, for auditing and evaluation purposes (Sayana, 2005; Tafti, 2005). As the outsourcing market matures, new risks emerge where uncertain information confidentiality and increased management complexity have become increasingly apparent. A high possibility of security issues abounds when a provider has to serve several direct competitors, which means having to maintain confidentiality about the information corresponding to all of them (Weakland, 2005; Grover, Cheon & Teng, 1994; Lacity & Hirschheim, 1993).

A survey conducted by the International Association of Outsourcing Professionals (IAOP) has revealed that the main problem facing modern businesses is that of IT security where 90 % of those interviewed said that a leak of confidential information that occurred during outsourcing would have catastrophic consequences for their companies (Tolle, 2006). Data privacy concerns are not only important because of legal obligations in the face of security breaches and consequent data leakage, but have public relations repercussions following the illegal disclosure of private information (Taherzadeh, 2007). Another issue is intellectual property (IP) which varies among organizations. The protection of IP is necessitated due to security concerns such as technical vulnerabilities and inappropriate leakage of IP (Musaji, 2005). Although a few client companies transfer only dummy data to their providers, yet it may be sufficient to interpret the data actually kept in the clients' database since the dummy data bear similarities to the real data. In addition, engaging outsource services for specific ICT core functions such as maintenance of database, network or even the system may be inappropriate as it could lead to the exposure of client information assets (Arshad et al., 2007). As vendors take control of IT functions, there are fears that providers may take advantage of clients while others also fear providers may not maintain confidentiality and privacy. Case incidents in print media have reported security breaches by providers or parties closely associated with providers that justify such concerns (Weiss, 2005; Collett, 2004; Costa, 2001). Clearly, companies that consider outsourcing must realize that there are negative consequences to such practices (Beulen et al., 2006).

The argument still stands that a company can better control its information assets when it is on-site than when such assets are in the possession of a provider, as it becomes much harder to protect (Kakumanu & Portanova, 2006). Unfortunately, outsourcing is becoming a salient trend in today's fast-moving information-rich digital economy. Thus, it is necessary to consider countermeasures to data leakage by reducing its risks in ICT outsourcing. It would be illogical to assume that by practicing such methods, data leakage could be eradicated in its entirety, as unpredictable and new risks coming from soft factors and new technologies must be factored in. However, this study has attempted to highlight the issue of these potent risks and has offered various countermeasures that companies contemplating outsourcing should seriously consider in order to protect their information assets.

RESEARCH METHODOLOGY

An empirical study using a questionnaire survey was applied in this research. The sampling method used to select the respondents for this research was judgment sampling which involved the choice of respondents who are most advantageously placed or in the best position to provide the information required. In this case, the target respondents were those involved in ICT outsourcing contracts within their respective organizations. Both primary and secondary data were used in order to achieve the objectives. ICT outsourcing inherent risks, and data privacy and security safeguards were compiled and examined from past research studies and other secondary resources. From this examination, the countermeasures to reduce data leakage risks were determined. An in-depth study was then conducted to determine the existence of concerns on data leakage in ICT outsourcing among Malaysian organizations.

Research Model

The research model in Figure 1 was designed to achieve the study objective of determining data leakage risks and countermeasures when outsourcing ICT services.

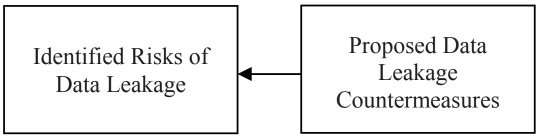
Identified Risks of Data Leakage
Proposed Data Leakage Countermeasures

Figure 1. Research Model of Data Leakage in ICT Outsourcing

The seventeen inherent risks listed in Table 1 were compiled from past research studies. The countermeasures to data leakage are provided in Table 2. As there appeared to be limited research studies (both international and local) concentrating on such countermeasures, resource materials from ICT practitioners were also referenced. Table 2 also contains the formulated hypotheses to examine positive associations of the methods to reducing data leakage risks. A model of the hypotheses is illustrated in Figure 2.

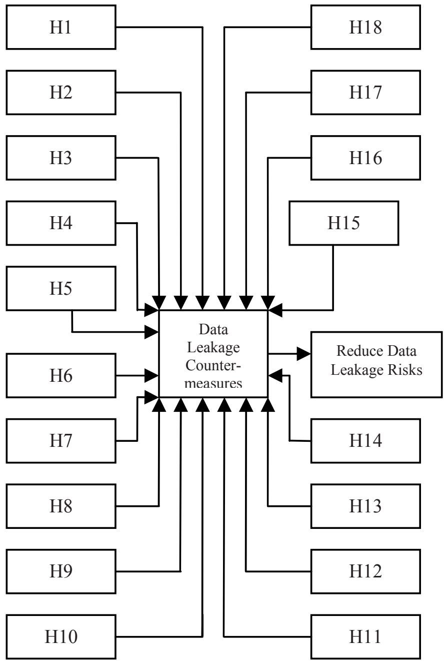

Figure 2. Hypotheses Model of Data Leakage Countermeasures

FINDINGS AND RESULTS

The survey questionnaire captured background data of the respondents' profiles as well as their opinions on ICT outsourcing inherent risks and data leakage countermeasures based on their respective work environments of the 100 sets of questionnaires that were distributed to public and private organizations, only 53 sets were returned. However, only 50 sets were completed and deemed suitable for analysis.

Demographic Profile

Some of the demographic characteristics examined included the respondent's position, organization status, organization's years of establishment, organization size, and outsource participation. Data analysis indicated that a majority of the respondents (66%) were IT/IS management and technical staff while the remainder (34%) comprised of senior management staff. The involvement of non-IT/IS personnel in ICT outsourcing was due to the absence of a proper IT department within some organizations. In the category of organization status, 54% of the sample were from public organizations with the remaining 46% coming from private organizations. About 62% of the respondents were from organizations established more than 10 years ago. while 30% were from organizations established between 5 to 10 years. All organizations represented by the sample have participated in ICT outsourcing during the course of their establishment and a majority (76%) has practiced it for at least 5 years. It would seem that maturing/matured organizations display a greater tendency to outsource their ICT functions while concentrating on their core competencies.

As for the size of the organization, it was found that 60% of the respondents were from organizations with more than 100 full-time staff with another 36% with 50 to 100 full-time staff. The size of these organizations may be considered medium to large (Saleh and Ndubisi, 2006; Hashim, 2000). This is consistent with the majority of the sample coming from public organizations which are generally large and concurs with the overall presence of ICT outsourcing due presumably to large budgets and increased ICT usage. The type of outsourcing services preferred by the respondent sample relate closely to organizational ICT infrastructure and solutions, with the most frequent services being application development (54%), network services (42%), and database service and operation (38%). Respondents were allowed to select more than one service from a list of 17 ICT outsourcing services.

Table 1

Ranking of Inherent Risks in ICT Outsourcing

Rank	Inherent Risk	Mean
1	The provider does not comply with the contract as stated in the service-level agreement (SLA) (Gonzalez et al., 2005; Claver et al., 2002).	4.20
2	Data confidentiality/privacy violation (Karyda et al., 2006; Gonzalez et al., 2005; Klosek, 2005; Tafti, 2005; Khalfan, 2004).	4.08

(continued)

Table 1

Ranking of Inherent Risks in ICT Outsourcing

Rank	Inherent Risk	Mean
3	An excessive dependence on the outsource provider (Hoecht and Trott, 2006; Tafti, 2005; Gonzalez et al., 2005).	4.04
4	Poor system quality (Sabherwal, 2003; Ross & Westerman, 2003).	3.92
5	Occurrence of data leakage/exposure to other parties (Hoecht and Trott, 2006; Karyda et al., 2006; Gonzalez et al., 2005; Khalfan, 2004).	3.88
6	Lack of protection for intellectual property rights (Karyda et al., 2006; Rosenthal, 2006; Ramanujan & Jane, 2006; Klosek, 2005; Musaji, 2005; Tafti, 2005).	3.50
7	Client lacks outsourcing experience to manage outsource relationship (Murphy, 2003).	3.38
8	Communication difficulties between client and vendor (Kim et al., 2005; Rao, 2004).	3.26
9	Hidden costs (Khalfan, 2004; Gonzalez et al., 2005; Carmel & Nicholson, 2005; Erber & Sayed-Ahmad, 2005; Claver et al., 2002; Wang, 2002; Barthe'lemy, 2001; Lee, 1996).	3.26
10	Client lacks outsourcing skills to manage outsource relationship (Murphy, 2003).	3.16
11	Unclear cost-benefit relationship (Khalfan, 2004).	3.02
12	Loss of critical skills and expertise among IT employees of client organizations when most tasks are done by the provider (Hoecht & Trott, 2006; Gonzalez et al., 2005; Tafti, 2005; Perrons & Platts, 2004).	2.94
13	Lack of integration between new and legacy applications (Salmela and Turunen, 2003).	2.82
14	The provider's staff lack experience to perform related tasks (Gonzalez et al., 2005; Sullivan & Ngwenyama, 2005; Claver et al., 2002; Gay & Essinger, 2000).	2.68
15	The provider's staff lack the qualification to perform related tasks (Gonzalez et al., 2005; Sullivan & Ngwenyama, 2005; Claver et al., 2002; Gay & Essinger, 2000).	2.66
16	Opposition from internal IT/IS staff who felt threatened due to possibility of organization reducing staff (Gonzalez et al., 2005; Claver et al; 2002).	2.60
17	Opposition from internal IT/IS staff due to increase in work load caused by technology development resulting from ICT outsourcing (Gonzalez et al., 2005; Claver et al; 2002).	2.58

Table 2

Methods (Countermeasures) to Reduce the Risk of Data Leakage

Method	Description	Reference	Hypothesis	
Outsourcer's experience	Investigate outsourcer's experience with data privacy and security.	Owens and Van Vuuren, 2007; Klosek, 2005; Musaji, 2005; Kim and Chung, 2003.	**H1:**	Investigating outsourcer's experience with data privacy and security **positively** reduces data leakage risk in ICT outsourcing.
Subcontract	Agree to subcontract only if the subcontractor will fully comply to existing obligations.	Klosek, 2005; Peterson, 2002.	**H2:**	Agreeing to subcontract only if the subcontractor will fully comply to existing obligations **positively** reduces data leakage risk in ICT outsourcing.
Encryption	Encrypt all data while in storage and during transit.	PGP, 2006; Henry, 2005.	**H3:**	Encrypting all data while in storage **positively** reduces data leakage risk in ICT outsourcing.
			H4:	Encrypting all data during transit **positively** reduces data leakage risk in ICT outsourcing.
Internal data audit	Conduct internal data audit of outsourced data to obtain complete knowledge.	Klosek, 2005; Sayana, 2005.	**H5:**	Conducting internal data audit of outsourced data to obtain complete knowledge **positively** reduces data leakage risk in ICT outsourcing.

(continued)

Table 2

Methods (Countermeasures) to Reduce the Risk of Data Leakage

Method	Description	Reference	Hypothesis
Required information	Allow only required information to perform the service to be accessed by outsource provider.	Henry, 2005.	**H6:** Allowing only required information to perform the service to be accessed by outsource provider **positively** reduces data leakage risk in ICT outsourcing.
Standards	Ensure the provider's physical and data security standards meet/exceed the client's requirements.	McKinney, 2005; Henry, 2005; Peterson, 2002.	**H7:** Ensure the provider's physical and data security standards meet/exceed the client's requirements **positively** reduces data leakage risk in ICT outsourcing
Contract agreement	Ensure the contract agreement addresses the provider's responsibility for security and confidentiality of client's resources and include confidential information definition and stipulation of penalties.	Karyda et al., 2006; Sayana, 2005; Benvenuto and Brand, 2005; Lee, 1996; Scott, 1996.	**H8:** Stateing confidential information definition and stipulation of penalties in contract agreement **positively** reduces data leakage risk in ICT outsourcing. **H9:** Addressing provider's responsibility for security and confidentiality of client's resources in contract agreement **positively** reduces data leakage risk in ICT outsourcing.

(continued)

Table 2

Methods (Countermeasures) to Reduce the Risk of Data Leakage

Method	Description	Reference	Hypothesis
Background checks	Conduct detailed background checks for provider's employees involved in outsourcing project.	McKinney, 2005; Henry, 2005; Peterson, 2002.	**H10:** Conducting detailed background checks for provider's employees involved in outsourcing project **positively** reduces data leakage risk in ICT outsourcing.
Disposal of data	Ensure the provider destroys/disposes all and unwanted outsourced data upon project completion, and this is monitored by the project manager (lead authority) of both parties.	Institute of Actuaries, 2009; University of Utah, 2007; Victoria University, 2006.	**H11:** Ensuring provider destroys/disposes unwanted outsourced data upon project completion **positively** reduces data leakage risk in ICT outsourcing. **H12:** Ensuring provider destroys/disposes all outsourced data upon project completion **positively** reduces data leakage risk in ICT outsourcing. **H13:** Project managers of both parties monitoring the disposal of outsourced data **positively** reduces data leakage risk in ICT outsourcing.

(continued)

Table 2

Methods (Countermeasures) to Reduce the Risk of Data Leakage

Method	Description	Reference	Hypothesis
Physically secured environment	Provider establishes physically secured environment and sufficient security precautions.	McKinney, 2005.	**H14:** Provider establishing physically secured environment and sufficient security precautions **positively** reduces data leakage risk in ICT outsourcing.
Regular checks	While projects are on-going, conduct regular checks within the organization and perform on-site visits at the provider's working place.	Tafti, 2005; McKinney, 2005; Leem and Lee, 2004.	**H15:** Performing on-site visits to provider's working place while projects are ongoing **positively** reduces data leakage risk in ICT outsourcing.
			H16: Performing regular checks when projects are ongoing and carried out within the organization **positively** reduces data leakage risk in ICT outsourcing.
Provider's policies	Periodically review the provider's policies relating to internal controls and security.	Tafti, 2005; Peterson, 2002.	**H17:** Periodically reviewing the provider's policies relating to internal controls and security **positively** reduces data leakage risk in ICT outsourcing.

(continued)

Table 2

Methods (Countermeasures) to Reduce the Risk of Data Leakage

Method	Description	Reference	Hypothesis
Meeting agenda	Place data confidentiality and privacy as a regular discussion during meetings between client and provider.	National Directors Institute, 2007; Owens and Van Vuuren, 2007; Foley, 2007.	**H18:** Placing data confidentiality and privacy as a regular discussion during meetings between client and provider **positively** reduces data leakage risk in ICT outsourcing.

Results of Reliability Test

Cronbach's alpha reliability test was used to establish the reliability of three measured items in the survey in terms of consistency and stability. A reliability coefficient, or Cronbach's alpha, that is closer to the value '1' is desired. Since all the measured items in Table 3 had a reliability of more than 0.7, the scales for these constructs were deemed to exhibit an adequate reliability.

Table 3

Results of Reliability Test

Measured Items	No. of Items	Cronbach's alpha
Inherent risks	17	0.829
Data leakage countermeasures	18	0.773

Results of Tests on Inherent Risks and Countermeasures

The results of the inherent risks (Table 1) were analysed and ranked from highest to lowest in order of importance by the mean scores. Based on the methods (countermeasures) in Table 2, attention is drawn to the inherent risks that are closely associated with data leakage which are (i) data confidentiality/ privacy violation (ranked 2nd), (ii) occurrence of data leakage/exposure to other parties (ranked 5th), and (iii) lack of protection for intellectual property (IP) rights (ranked 6th).

The Bivariate Pearson Product-Moment Correlation test was administered on the formulated hypotheses and the results of the hypothesis tests indicated positive correlations for all 18 hypotheses that were tested (Table 4). The output also indicated that the associations between the methods/countermeasures and the reduction of data leakage in ICT outsourcing are significant. While 14 hypotheses results showed moderate positive associations, hypotheses H6, H11, H12, and H13 showed strong positive associations. Overall, the implication clearly leans to a higher reduction in data leakage risks with higher applications of these countermeasures. Aside from the four hypotheses results that showed strong significant associations, the remaining fourteen hypotheses showed moderate positive associations.

Table 4

Results of Research Hypothesis Tests of Reducing Data Leakage Risk in ICT Outsourcing

Hypothesis	**Correlation Coefficient**	***p-value***	**Decision**	**Finding**
H1	0.438	.001*	Significant	Moderate, positive association
H2	0.652	.000*	Significant	Moderate, positive association
H3	0.462	.001*	Significant	Moderate, positive association
H4	0.462	.001*	Significant	Moderate, positive association
H5	0.621	.000*	Significant	Moderate, positive association
H6	0.742	.000*	Significant	Strong, positive association
H7	0.491	.000*	Significant	Moderate, positive association
H8	0.690	.000*	Significant	Moderate, positive association
H9	0.394	.005*	Significant	Moderate, positive association
H10	0.521	.000*	Significant	Moderate, positive association
H11	0.732	.000*	Significant	Strong, positive association
H12	0.738	.000*	Significant	Strong, positive association
H13	0.708	.000*	Significant	Strong, positive association
H14	0.339	.016*	Significant	Moderate, positive association
H15	0.466	.001*	Significant	Moderate, positive association
H16	0.448	.001*	Significant	Moderate, positive association
H17	0.680	.000*	Significant	Moderate, positive association
H18	0.377	.007*	Significant	Moderate, positive association

**Significant at 0.05 level*

DISCUSSION

The high ranks of importance attained by the three inherent risks (i.e., data confidentiality violation, occurrence of data leakage to other parties and lack of protection for IP rights) are in support of the high priority given to the loss of data confidentiality among Arab Gulf nations when public and private organizations engage or contemplate outsourcing (Khalfan, 2004; Badri, 1992). These risks, which are closely associated with data leakage, are critical issues that both the client organization and the provider must take into account as a matter of good professional practice during outsourcing arrangements. The obligations, restrictions and jurisdiction under which both parties operate must be addressed as legal and regulatory frameworks that may be involved must be defined in case of disputes. Data privacy and security, and protection of IP rights that arise from these arrangements must be clearly laid down within the respective contractual agreements (Karyda et al., 2006; Klosek, 2005; Tafti, 2005).

The client company can reduce the possibility of data leakage risk during outsourcing by allowing only information required to perform the service to be accessed (H6) and used by the service provider in the outsourcing activity, thereby limiting the provider's access to organization data. Data is also compromised in the event an improper disposal occurs and can be subsequently leaked to other interested parties, thereby placing the credibility of clients' businesses at stake. Precautionary measures must be undertaken upon project completion to ensure that all outsourced data including unwanted sensitive outsourced data are destroyed or disposed by the provider (H11 and H12). These countermeasures prevent the reuse of sensitive data for purposes other than what it was intended and also prevent the misuse of data if kept in their possession. Data leakages in this manner can damage and impact the client company's business operation, profitability, or reputation, even exposing the company to legal action. The sample respondents seemed strongly inclined to having the project managers (or lead authorities) of the provider and the client monitor the disposal of the outsourced data (H11 and H12). By ensuring that the respective lead authority of each party supervises the disposal (H13), the accountability is thus held by these individuals to reliably seal possible data leakages upon project completion. These findings are in line with reports from local practitioners on the importance of data disposal and ensuring that the disposal process is done properly (Fernandez, 2010; Bernama, July 13, 2005).

There are optimistic expectations of data leakage risks being reduced with the application of countermeasures. However, the moderate nature of some correlations does raise questions as to the enforcement issue of the countermeasures to reduce risks, as respondents found data leakage risk to be significant and yet a majority of these countermeasures must have been in place judging from the duration of time ICT outsourcing has been practiced by the data sample.

CONCLUSION

The main objectives of this study were to identify the data leakage risks and to determine countermeasures to reduce such risks in ICT outsourcing. From the findings, it was apparent that the inherent risks of data leakage were significant to the respondent sample and that the countermeasures were positively correlated to reducing the risks. The results of this study indicate the current situation of data leakage risks faced and the countermeasures adopted by practitioners among some Malaysian organizations. However, more effort is required to enforce the routine of these countermeasures as precautionary procedures to safeguard data privacy and security. The diversity (or absence thereof) of individual laws and regulations when dealing with outsourcing among foreign countries will hinder the protection of data confidentiality (Tafti, 2005). Nevertheless, the enactment of such laws is a positive sign. On a final cautionary note, Hoecht and Trott (2006) contend that data leakage may be difficult to detect, let alone prove, and that the commercial damage may not be compensated with any legal redress.

REFERENCES

Arshad, N. H, Yap, M. L., & Mohamed, A. (2007). ICT outsourcing: Inherent risks, issues and challenges. *World Scientific & Engineering Academy & Society (WSEAS) Journal on Business and Economics, 4*(8), 117–125.

Badri, M. (1992). Critical issues in information systems management: An international perspective. *International Journal of Information Management, 12*, 179–191.

Bakalov, R., & Nanji, F. (2005). Offshore application development done right. *Information Systems Control Journal, 5*.

Barthe´lemy, J. (2001). The hidden cost of IT outsourcing. *MIT Sloan Management Review, 42*(3), 60–9.

Benvenuto, N. A., & Brand, D. (2005). Outsourcing - A risk management perspective. *Information Systems Control Journal, 5*.

Bernama. (2010, February 4). *Outsourcing sector revenue to grow by 20–25 percent this year*. Bernama.com. Retrieved from www.bernama.com

Bernama. (2005, July 13). *Not all companies following proper data destruction procedures*. Bernama.com. Retrieved February 25, 2010 from www.bernama.com

Beulen, E., Ribbers, P., & Roos, J. (2006). *Managing IT outsourcing*. Routledge. Taylor & Francis Group.

Carmel, E., & Nicholson, B. (2005). Small firms and offshore software outsourcing: High transaction cost and their migration. *Journal of Global Information Management, 13*(3), 33–54.

Claver, E., Gonzalez, R., Gasco, J., & Llopis, J. (2002). IT outsourcing: Reasons, reservations and success factors. *Logistic Information Management, 15*(4), 294–308.

Collett, S. (2004, March 15). Outsourcing: Losing control. *Computerworld.* Retrieved from http://www.computerworld.com/

Costa, C. (2001). Information technology outsourcing in Australia: A literature review. *Information Management & Computer Security*, *9*(5), 213–224.

Dhar, S., & Balakrishnan, B. (2006). Risks, benefits and challenges in IT outsourcing: Perspectives and practices. *Journal of Global Information Management*, *14*(3), 39–69.

Erber, G., & Sayed-Ahmed, A. (2005). Offshore outsourcing: A global shift in the present IT industry. *Intereconomics*, *40*(2), 100–12.

Fernandez, C. (2010, April 5). Tasked to destroy old government data. *The Star: StarMetro,* pp. M5 and *CyberSecurity Malaysia (News)*. Retrieved from www.cybersecurity.my.

Foley, M. F. (2007, August). Board oversight of information technology, data privacy & data security: The New Imperative. *IBLS Internet Law - News Portal.* Wisconsin Lawyer Magazine.

Gay, C. L., & Essinger, J. (2000). *Inside outsourcing: The insider's guide to strategic sourcing.* London.

Gonzalez, R., Gasco, J., & Llopis, J. (2005). Information systems outsourcing risks: A study of large firms. *Industrial Management and Data Systems*, *105*(5), 45–62.

Grover, V., Cheon, M. J. & Teng, T. C. (1994). A descriptive study on the outsourcing of information systems functions. *Information & Management*, *27*(1), 33–44.

Hashim, M. K. (2000). SME's in Malaysia: Past, present and future. *Malaysia Management Review*, *35*(1), 22–30.

Henry, P. (2005). How to keep data safe when outsourcing offshore. *ComputerWorld.* Retrieved from http://www.computerworld.com/

Hoecht, A. & Trott, P. (2006). Outsourcing, information leakage and the risk of losing technology-based competencies. *European Business Review*, *18*(5), 395–412.

Institute of Actuaries. (2009, September). Data security. *DPB Compliance Bulletin No. 21*.

Kakumanu, P. & Portanova, A. (2006). Outsourcing: Its benefits, drawback and other related issues. *Journal of American Academy of Business, 9*(2), 1–7.

Karyda, M., Mitou, E., & Quirchmayr, G. (2006), A framework for outsourcing IS/IT security services, *Information Management & Computer Security*, *14*(5), 402–415.

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

Kim, S., & Chung, Y. (2003). Critical success factors for IS outsourcing implementation from an international relationship perspective. *Journal of Computing Information Systems, 43*(4), 81–90.

Kim, J. W., Meso, P., & Kim, D. G. (2005, December). *Cultural effects on offshore-outsourced systems development*. Paper presented at the 13th Annual Cross-cultural Meeting in Information Systems. Las Vegas, Nevada, U.S.A.

Klosek, J. (2005). Data privacy and security are a significant part of the outsourcing equation. *Intellectual Property and Technology Law Journal, 17*(6), 15–18.

KPMG (2004). *Information risk management Asia Pacific outsourcing survey*. Retrieved from www.kpmg.com.au.

Lacity, M. C. & Hirschheim, R. A. (1993). Implementing information systems outsourcing: Key issues and experiences of an early adopter. *Journal of General Management, 19*(1), 17–31.

Lee, Y. C. (2010, June 10). Protecting personal data. *The Star*.

Lee, M. K. (2009, May 29). Malaysia keeps lofty spot for global services. *ZDNet Asia*.

Lee, M. K. O. (1996). IT outsourcing contracts: Practical issues for management. *Industrial Management and Data Systems, 96*(1), 15–20.

Leem, C., & Lee, H. (2004). Development of certification and audit processes of application service provider for it outsourcing. *Technovation*, *21*(1), 63–72.

McKinney, C. (2005). Capability maturity models and outsourcing: A case for sourcing risk management. *Information Systems Control Journal*, *5*.

Murphy, J. (2003). Ways to evaluate and address your outsourcing risk. *Gartner Research.*

Musaji, Y. (2005). Sarbanes-Oxley and business process outsourcing risk. *Information Systems Control Journal*, *5*.

National Directors Institute (2007). *Board oversight of data privacy and security.* Foley & Lardner LLP.

Owens, R., & Van Nuuren, F. (2007, July). Privacy law and outsourcing in Canada. *Blakes Bulletin on Privacy & Outsourcing*, 1–12. Blake, Cassels & Graydon LLP.

Perrons, R. K., & Platts, K. (2004). The role of clockspeed in outsourcing decisions for new technologies: Insights from the prisoner's dilemma. *Industrial Management & Data Systems*, *104*(7), 624–32.

Peterson, B. L. (2002). Information security in outsourcing arrangements. *Outsourcing Journal.* Retrieved from http://www.outsourcing -journal.com/

PGP (2006). Affiliated computer services, inc. (ACS): Securing sensitive data in business process outsourcing. *ACS Case Study*. PGP Corporation.

Rao, M. T. (2004). Key issues for global IT sourcing: Country and individual factors. *Information Systems Management, 21*(3), 16–21.

Ramanujan, S., & Jane, S. (2006). A legal perspective on outsourcing and offshoring. *Journal of American Academy of Business*, *8*(2), 51.

Rosenthal, B. E. (June, 2006). Booz Allen Hamilton Study: Data security is becoming a distinguishing factor when selecting a supplier. *Outsourcing Journal.* Retrieved from http://www.outsourcing-journal.com/jun2006-boozallen.html

Ross, J. W. & Westerman, G. (2003). Architecting new outsourcing solutions: The promise of utility computing, *Massachusetts Institute of Technology Center for Information Systems Research*, CISR WP 117 and Sloan WP No. 4458–01.

Sabherwal, R. (2003). The evolution of coordination in outsourced software development projects: A comparison of client and vendor perspectives. *Information and Organization*, *13*, 153–202.

Saleh, A. S., & Ndubisi, N. O. (2006, August). An evaluation of SME development in Malaysia. *International Review of Business Research Papers, 2*(1), 1–14.

Salmela, H., & Turunen, P. (2003). Competitive implication of IT In the public sector: The case of a city GIS. *International Journal Of Public Sector Management, 16*(1), 8–26.

Sayana, S. A. (2005). Auditing IT service delivery. *Information Systems Control Journal*, *5*.

Scott, Y. (1996). Audit and control of information services outsourcing. *Information Systems Control Journal*, *6.*

Sullivan, W.E., & Ngwenyama, O. K. (2005). How are public sector organizations managing IS outsourcing risks? An analysis of outsourcing guidelines from three jurisdictions. *Journal of Computer Information Systems, 45*(3), 73–87.

Tafti, M. H. A. (2005). Risks factors associated with offshore it outsourcing. *Industrial Management & Data Systems, 105*(5), 549–560.

Taherzadeh, M. (2007). Worldwide: Privacy and outsourcing: Evolving concerns. *Mayer Brown LLP*. Retrieved from www.mondaq.com/

Tolle, S. (2006). Confidential data leaks during outsourcing tantamount to Bankruptcy. *Infowatch*. Retrieved from http://www.infowatch.biz/

Turban, E., King, D., & Lang, J. (2009). *Introduction to electronic commerce* (2nd ed.). International Edition. Pearson Education, Inc.

University of Utah. (2007, March). *Standard for electronic media disposal.* University of Utah.

Victoria University. (2006, July). *Policies and associated procedures for the disposal and cleansing of IT equipment.* Victoria University.

Vijayan, J. (2006, June 1). Two more organizations report data breaches, *Computerworld*. Retrieved from http://www.computerworld.com/

Wang, E. T. G. (2002). Transaction attributes and software outsourcing success: An empirical investigation of transaction costs theory. *Information Systems Journal, 12*, 121–152. In Dhar, S. and Balakrishnan, B. (2006). Risks, benefits, and challenges in global IT outsourcing: Perspectives and practices. *Journal of Global Information Management, 14*(3), 39–69.

Weakland, T. (2004). *2005 Global IT outsourcing study.* DiamondCluster International, Inc.

Weiss, T. R. (2005, July 20). Visa, Amex cut ties with processing firm hit by security breach. *Computerworld*. Retrieved from http://www.computerworld.com/