ICT Outsourcing Information Security Risk Factors: An Exploratory Analysis of Threat Risks Factor for Critical Project Characteristics

Nik Zulkarnaen Khidzir
Infrastructure University Kuala Lumpur, Faculty of Information and Computing Technology, Kuala Lumpur, Malaysia
nikz@iukl.edu.my

Azlinah Mohamed and Noor Habibah Arshad
Universiti Teknologi MARA, Faculty of Computer and Mathematical Sciences, Shah Alam, Malaysia
azlinah@tmsk.uitm.edu.my, habibah@tmsk.uitm.edu.my

***Abstract*—ICT outsourcing is one of the successful strategies implemented to reduce organization's ICT operational cost and to give more priority to their core business rather to ICT operational activities. However, it causes significant risks to the success of the outsourcing ventures especially Information Security Risk (ISR). Therefore, analysis of ISR factors level for ICT Outsourcing project is required to prepare appropriate plan in order to minimize the impact of the risk to organization. The objective of this study is to assess the information security Threat Risks Factor (TRF) severity level for ICT Outsourcing project characteristics through exploratory analysis approach. Questionnaires were distributed to 300 private companies from various industry and government agencies in Malaysia involved in ICT Outsourcing projects. The project characteristics such Projects Type; Number of Service Provider; Outsourcing Strategy, Outsourced Project Percentage; Project Duration; Project Cost; and Project Team Size were analyzed. Thus, TRF severity levels were discovered for ICT outsourcing project characteristics commonly implemented in Malaysia. Results of the analysis reveal the evidence of highly risk ICT outsourcing project characteristics exploited through TRF. Hence, the organization could be able to avoid these ICT outsourcing project profile characteristics in order to minimize the risk and its related impacts. Finally, organizations can re-evaluate potential risks and improve their practices managing information security risk and urgently address information security risks to gain optimum benefits from their ICT outsourcing ventures.**

***Index Terms*—ICT Outsourcing, Information Security, Threats Risk Factor, Project Characteristics, Exploratory Analysis**

I. Introduction

The ICT outsourcing strategy is widely associated with cutting costs, launching of new business ventures and improving efficiency. However, the literatures have emphasized the risks associated with ICT outsourcing project implementation and identifying information security risks is one of the critical risks in the process [1, 2]. Thus, it is crucial to manage ISR because it could cause failure to ICT services and security of the information asset in organizations. Therefore, exploratory analyses on ICT outsourcing information security risk factors are crucial to diagnose the severity of the risk among organization in Malaysia. This paper explores the Threat Risk Factor severity level for ICT outsourcing project characteristics which were commonly implemented in Malaysia. The findings could assist in planning and decision making preparing more effective information security management plan.

Manuscript received July 19, 2013; revised September 20, 2013.

II. Literature Review

A. Information Security Core Principles

Information security involves the activities, processes, controls and efforts that aim to protect information and data, and their underlying infrastructures. Confidentiality, integrity and availability are the core principles of information security [3]-[5] and broadly used in most study fields [6]. Confidentiality refers to the limitations on the use and retention of different kinds of information [3], [4], [7], [8]. Integrity is the guarantee that information has not been manipulated [3], [4], [7], [8] while availability is ensuring that authorized users have access to information and associated assets when required [3], [4], [7], [8]. Information security issues and its associated risk should be thoroughly considered from various perspectives in ICT outsourcing project implementation. Additionally, associated ICT risk factors that contribute to the information security incident through outsourcing ventures should be evaluated further to reduce negative impact to organization.

B. Information Security Risks Factor for ICT Outsourcing

Information Security Risks are chances of threats action on vulnerabilities to cause impacts contributed to information security incidents [2]. Information security risks are theft of personal data, information leakage, extraction or loss and unauthorized exploitation of

doi: 10.12720/jiii.1.4.218-222

intellectual properties. These risks are caused by lack of control on threats and vulnerabilities. Threats refer to natural or man-made circumstance or event that could have an adverse or undesirable impact, minor or major, on organizational asset [2], [9], [10]. Vulnerabilities refer to the absence or weaknesses of a safeguard in an asset that makes a threat potential more harmful or costly, more likely to occur, or likely to occur more frequently [2], [9], [10]. Risk factors refer to any factors that influence the undesirable events that may occur in organizations [11], [12]. For ICT information security, a similar risk factor concept was adopted into information security for ICT project implementation. Failure of ICT outsourcing projects is commonly attributed to information security risks.

Prior literature has highlighted four factors that contribute to information security risk for ICT Outsourcing project implementation, Threat Risks Factor (TRF); Vulnerability Risks Factor (VRF); Information Security Management Defect Risks Factor (ISMDRF); and Challenges Managing Unexpected Change Risks Factor (CMUCRF) [13]. However, the study emphasizes the exploratory analysis on Threat Risks Factor (TRF) severity levels for ICT outsourcing project characteristics. The results were measured and statistically analyzed to measure the severity of the risks factor.

C. ICT Outsourcing Project Implementation and Significant Risks

ICT outsourcing strategy involves transferring some or all of the ICT related decision making rights, business processes, internal activities and services to external providers who develop and administer these activities in accordance with the deliverables, performance standard and outputs, as agreed in a contractual agreement [14]. The literature has highlighted various ICT related projects commonly outsourced to external providers. Many organizations outsource their ISP services, web hosting, e-business solutions, ICT application maintenance and support, software application services provision, application analysis, ICT infrastructure development, programming, support end-user, staff/user training courses, ICT security audit and security policy consulting or standards development [15], [16]. Despite the varying categories, the outsourcing processes or cycle remain almost similar. The generic conceptual phases of ICT outsourcing cycle as illustrated in Fig. 1 are; the analysis of decision to outsource; selection of Service Providers; contract management and project on-going monitoring [17]. Organizations adopt the outsourcing strategy in their ICT projects as it plays a significant role in reducing ICT operational costs [18] and improving the efficiency of their ICT services whilst enabling them to focus on the core businesses. Unfortunately, outsourcing suffers from many potential risks [19] that must be recognized and managed [20] effectively. Recent studies reveal that information security risks are amongst the highest risks in ICT outsourcing project [1], [2] that need to be addressed to ensure maximum benefit.

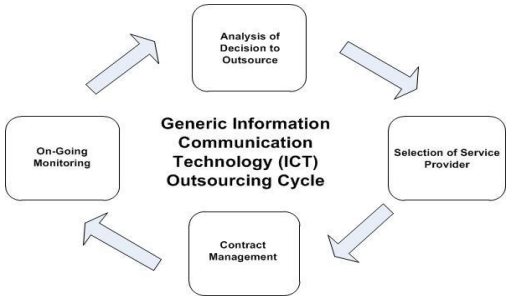

Figure 1. Generic ICT Outsourcing Phases Implementation [17]

Failure of ICT outsourcing projects and its implementation were commonly attributed to information security risks. Table I highlight several literatures on the information security risks related to the ICT outsourcing cycle.

TABLE I. ICT OUTSOURCING PHASES AND INFORMATION SECURITY RISKS

ICT Outsourcing Lifecycle	Information Security Risks (ISRs)	Reference Literatures
Analysis of Decisions to Outsource	Information Leakage, Poor Information Security Study	[2],[21],[22]
Selection of Service Provider	Unauthorized Exploitation of Intellectual Property Right (IPR)	[2],[23],[24],[25]
Contract Management	Information Leakage	[2],[22]
On-Going Monitoring	Environmental Disaster, Information Leakage	[2],[26],[27],[28]

In order to allow a detailed analysis of the problem, the majority of ICT outsourcing project characteristics need to be assessed. For the purpose of this study, Threats Risk Factor level were analyzed to determine the risks factor severity in most of the ICT outsourcing project characteristics implemented in Malaysia.

III. METHODOLOGY

The analysis was conducted to determine Threats Risk Factors level for each ICT Outsourcing project characteristics among private and public agencies in Malaysia. Five-Point-Likert-Scale was used to measure the severity of Threat Risks Factor (TRF). Primary data was collected using survey questionnaires. Purposive sampling technique [29] was applied to collect primary data through electronic and postal mail to 300 respondents. The 36% response rate (110 respondents) was considered to be relatively normal [30] and acceptable to represent a sample population of the study. Analysis of primary data was supported by the application of appropriate statistical techniques.

A research model (Fig. 2) was developed to analyze the TRF severity level for seven common characteristic of ICT Outsourcing project implementation. The exploratory analyses the following project characteristics: Application System Development project that outsource to more than one service provider; implement join

venture outsourcing strategy; outsourced > 75% of their ICT functions; implemented between one to three years; with project cost between 1 Million to 5 Million and consist of medium size project team structure. Then, percentages of Threat Risks Factor (TRF) severities for three categories (Low: Between 1 and < 2.5; Medium: Between > 2.5 and < 3.5; High: > 3.5 and < 5) were evaluated in this study.

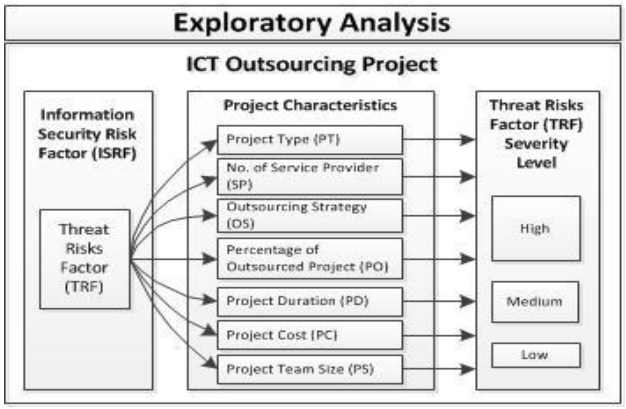

Figure 2. Research Model for Exploratory Analysis

IV. Results and Discussions

The results of the study captured the respondents' demographic profile, project characteristics descriptive analysis and their opinions on the level of Threat Risks Factor (TRF) for seven common ICT Outsourcing project characteristics. The analyses lead to several significant discoveries and expansion of existing knowledge.

A. Respondents Demographic Profiles Analysis

ICT project managers and senior information system officers from various industries and government agencies participated in this study. Only 18.2% respondents had working experience < 5 years. The other 81.8% respondents > 5 years' experience in ICT project. 15.5% of those had 11 to 15 years as well as 15 to 20 years' experience. The majority, 40.9%, had been working for 6 to 10 years. Respondents' demographic profile analysis results show the questionnaires were appropriately distributed to relevant respondents.

B. ICT Outsourcing Project Descriptive Analysis

The majority of respondents were from government agencies (79.1%), 11.7% from government-linked companies (GLCs) and 9.1% from private companies. Nevertheless, the 79.1% government agencies respondents represented numerous businesses and industrial sectors. The ICT outsourcing projects' characteristic analysis revealed that 57.3% of the projects concerned Application System Development, ICT Infrastructure Maintenance (26.4.3%), IT/IS Strategic Planning Results (6.4%), ICT Security Maintenance (5.5%), ICT Knowledge Transfer & Training (2.7%) and ICT Application Maintenance at 1.8%. Results revealed that Joint-Venture-Outsourcing (43.6%) was the most popular outsourcing strategy practiced in ICT project implementation among Malaysia organizations. Selective outsourcing approach accounted for 30.9% and Total outsourcing approach, 25.5%. For the majority (16.7%), the main reason for outsourcing ICT projects was the lack of internal resources and human expertise. The study also found out that most of the organizations outsource their ICT projects to only one service provider (58.2%). Most of the project durations were medium-term being between 1 to 3 years (62.7%), while short-term (less than 1 year) and long-term (more than 3 years) represented 18.2% and 19.1% respectively. Responses received from organizations were overwhelming with ICT outsourcing projects costing between RM 1 Million to RM 5 Million (23.6%). Descriptive analysis results highlighted the majority of the ICT outsourcing project characteristics implementation in Malaysia. Therefore, further analyses of TRF severity level were conducted to those ICT Outsourcing project characteristics.

C. Exporatory Analysis Results: Information Security Threat Risks Factor

Information Security Threats Risk Factor (TRF) was analyzed according to ICT outsourcing project characteristics (project type, no. of service providers, outsourcing strategy, percentage of outsourced projects, project duration, project cost and project team size). The results revealed the severity of the risk factor levels for the majority of the ICT outsourcing project implementation in Malaysia. The TRF severity level outlined in Table II is driven by results from 110 respondents who were directly involved in ICT outsourcing projects.

Results from Table II determine that Application System Development project that outsource to more than one service provider, implementing join venture outsourcing strategy, outsourced > 75% of the ICT functions, project duration between one to three years, project cost between 1 Million to 5 Million and medium size of project team were considered highly critical exposed to information security TRF. The highest severity TRF realized by majority of the respondent was medium size ICT outsourcing project. Conversely, only 10.9% of the respondent aware that ICT outsourcing project cost between RM 1Million to RM 5 Million were highly risk exposed to information security risks that contributed by TRF.

Majority of 57.3% TRF were found in Application System Development outsourcing project. Deeper analysis revealed that 27.3% reported it as a highly severe factor, 20.9% regarded it as moderately severe and only 9.4% was reported as low severe. Due to the highly critical TRF associated with Application Systems Development outsourcing projects, information security experts and practitioners are therefore required to give more attention to information security issues. The results also revealed that the TRF was more critical when ICT projects were outsourced to more than one outsourcing party. The total percentage of TRF when ICT projects involved more than one outsourcing parties was 51.8% compared to 48.2%, for a single outsourcing party. Result from exploratory analysis discovered that 30%

claimed it as a highly critical factor, 16.4% regarded it as moderately critical and only 5.5% was reported as low. This signifies there was difference in severity TRF levels with the number of service providers (SPs) involved in ICT outsourcing projects.

TABLE II. THREATS RISK FACTOR SEVERITY LEVELS BY ICT OUTSOURCING PROJECT CHARACTERISTICS

Project Characteristics/ Majority Project Criteria's		N (%)	Threats Risk Factor (TRF)			
			L (%)	M (%)	H (%)	Total (%)
PT	Application System Development	110	9.1	20.9	27.3	57.3
SP	> 1 No. of Service providers	110	5.5	16.4	30.0	51.8
OS	Join Venture Outsourcing	110	6.4	14.5	22.7	43.6
PO	> 75% Outsourced ICT Project	110	1.8	13.6	20.0	35.5
PD	Medium-Term (1 to 3 Years)	110	7.3	21.4	32.7	61.8
PC	Between RM 1 Million to RM 5 Million	110	4.5	8.2	10.9	23.6
PS	Medium Size (10 to 99)	110	6.4	28.2	36.4	70.9

L – Low Severity M – Moderate Severity
H – High Severity N – Percentage of Respondents
SP – No. of Service Providers OS – Outsourcing Strategy
PD – Project Duration PC – Project Cost
PS – Project Team Size PT – Project Type
PO – Percentage of Outsourced Projects

In view of the organization's outsourcing project strategy or outsourcing relationship types, the results revealed highly critical TRF for ICT projects implementing Joint-Venture outsourcing strategy (43.6%). Further analysis explored that 22.7% considered it as a highly critical factor, 14.5% regarded it as moderately critical and only 6.4% was reported for low critical. Hence, Joint-venture outsourcing strategy required more information security risk management efforts compared to other outsourcing strategies. This may be attributed to the complexity of joint-venture relationships which are often hampered by conflict of interests among involved parties.

Highly critical TRF (35.5%) was indicated when organizations outsource more than 75% of their ICT functions. The analysis revealed that 20% reported it as a highly critical factor, 13.6% regarded it as moderately critical and only 1.8% was reported for low critical. Meanwhile, 61.8% was indicated medium-term ICT outsourcing project duration contributed to high severity of TRF. The results revealed that 32.7% reported it as a highly critical factor, 21.4% regarded it as moderately critical and only 7.3% was reported for low critical.

The organizations' preference for medium-term ICT outsourcing project duration compared to long-term duration may be due to the rapid changes in ICT and the market environment. Thorough analysis revealed that 36.4% reported it as a highly critical factor, 28.2% regarded it as moderately critical and only 6.4% was reported for low critical. With this stated preference, organizations should urgently address the highly critical TRF in medium term projects in order to gain maximum benefits through their outsourcing ventures.

Subsequent, ICT outsourcing projects that cost between RM1 million and RM5 million were considered the highest total threats risk factor by 23.6% of the population. 10.9% indicated it as a highly critical threats risk, 8.2% as medium critical threats risk and 4.5% indicated it as low critical threats risk for ICT outsourcing projects. Meanwhile, the majority of TRF originated from the medium project team size. The exploratory analysis discovered that 36.4% reported it as a highly critical factor, 28.2% regarded it as moderately critical and only 6.4% was reported for low critical. Therefore, medium sized projects must prioritize information security management efforts since they are implicated as one of the most critical threats involved in medium sized ICT outsourcing projects.

V. CONCLUSION

The majority of respondents claimed that there was a high Threat Risks Factor (TRF) in their ICT outsourcing projects. Highly critical ICT outsourcing project characteristics based on the TRF exploratory analysis were discovered. Further analysis discovered TRF severity pattern were high for common ICT Outsourcing characteristics in Malaysia. The findings enable ICT professionals, information security experts and outsourcing practitioners to prioritize information security risk and project management issues effectively. Findings recommend that organizations required a sufficient resources allocation on information security aspects related to TRF for their ICT outsourcing project. Therefore, these findings could assist ICT security professional to prepare an appropriate mitigation plan strategically for their ICT outsourcing project. Finally, organization could get optimum benefit in their ICT outsourcing strategy and simultaneously minimizing associated impacts caused by information security risks.

ACKNOWLEDGMENT

The authors wish to thank RMI, UiTM and MOSTI for the research grant. Special thanks to the Faculty of Information Computing Technology, Infrastructure University Kuala Lumpur for the sponsorship to participate in ICFIT 2013.

REFERENCES

[1] D. Davison. (December 2003). Top 10 Risks of Offshore Outsourcing. [Online]. Available: http://techupdate.zdnet.com

[2] G. Hinson. (December 2007). Top Information Security Risk for 2008: Information Security Risk, CISSP Forum. [Online]. pp. 5. Available: http://www.naavi.org/cl_editorial_08/Top_information_security_risks_for_2008.pdf

[3] A. Vorster and Les Labuschagne, "A framework comparing different information security risk analysis methodology," in *Proc. South African Institute of Computer Scientist and Information Technologist on IT Research in Developing Countries*, 2005, pp. 95-103.

[4] Donn B. Parker, *Toward a New Framework for Information Security*, *Computer Security Handbook, 4th ed.*, edited by Seymour Bosworth and M. E. Kabey. New York: John Wiley & Sons, 2002.

[5] Wikipedia, The Free Encyclopedia. (January 2010). Information Security: Basic Principles, Key Concepts. [Online]. Available: www.wikipedia.org
[6] N. Z. Khidzir, A. Mohamed, and N. H. Arshad, "Critical information asset security requirements in ict outsourcing," in *Proc. International IT and Society Conference 2010*, vol. 1, no. 1, pp. 88-95.
[7] Code of Practice for Information Security Management, ISO17799:2005, ISO Standard –2005
[8] V. A. Canal, "The global voice of information security: On information security paradigms," *The ISSA Journal*, September 2005.
[9] R. Kaplan, "A matter of trust" in *Information Security Risk Management Handbook*, CRC Press, 2005, pp. 733.
[10] *The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM)*, MAMPU, Perpustakaan Negara Malaysia, 2005.
[11] B. A. Aubert, M. Patry, and S. Rivard, "A framework for information technology outsourcing risk management," *The Database for Advances in Information Systems*, vol. 36, no. 4, 2005.
[12] M. Levin and M. Schneider, "Making the distinction: Risk management, risk exposure," *Risk Management Journal*, vol. 44, no. 8, pp. 36-42, 1997.
[13] N. Z. Khidzir, N. H. Arshad, and A. Mohamed, "An exploratory factor analysis on information security risk in ict outsourcing," *Journal of Information Retrieval and Knowledge Management*. vol. 1, pp. 28-45, 2011.
[14] S. Dhar and B. Balakrishnan, "Risk, benefits and challenges in global IT outsourcing perspective and practices," *Journal of Global Information Management*, vol. 14, no. 3, pp. 39-69, 2006.
[15] NISER, Information Security Management System (ISMS) Survey, 2003.
[16] N. H. Arshad, Y. May-Lin, A. Mohamed, and S. Affandi, "Inherent risks in ICT outsourcing project," in *Proc. 8th WSEAS Conference*, 2007, vol. 8, pp. 141-146.
[17] S. Ruzaini H. S. Aris, N. H. Arshad, and A. Mohamed, "Conceptual framework of risk management in IT outsourcing project," *WSEAS Transactions on Information Science & Applications*, vol. 5, no. 4, pp. 816-831, 2008.
[18] Investopedia Dictionary. (January 2013). Definition of Outsourcing. [Online]. Available: http://www.investopedia.com
[19] N. Z. Khidzir, A. Mohamed, and N. H. Arshad, "Information security risk factors: Critical threats and vulnerabilities in ict outsourcing," in *Proc. International Conference on Information Retrieval and Knowledge Management*, March 2010, pp. 193-198.
[20] P. O'Keeffe and S. Vanlandingham, "Managing the risks of outsourcing: A Survey of Current Practices and their Effectiveness," *Protiviti Inc.*, 2004.
[21] M. Merkow and J. Breithaupt, "Securing information assets," in *Information Security Principles and Practices*, Prentice Hall, 2005, pp. 27.
[22] S. Garfinkel, "All your data belongs to us: Data servicing in another problem for data privacy," *Technology Review*, 2007.
[23] M. S Ju, S. K. Kim, and T. H. Kim, "A study on digital media security by hopfield neural network," *Lecture Note in Computer Science: Advances in Neural Networks*, p. 140. 2007.
[24] T. J. Sota, "Plagiarism in the age of electronic publishing," *Population Ecology*, vol. 46, no. 3, pp. 219, 2004.
[25] B. Vassiliadis, V. Fotopoulos, A. Ilias, and A. N. Skedras, "Protecting intellectual property right and the JPEG2000 coding standards," *Advanced in Informatics*, vol. 3746, pp. 705-715, 2005.
[26] S. Halliday, S. Badenhorts, and V. Solms, "A business approach to effective information technology risk analysis and management," *Information Management and Computer Security*, vol. 4, no. 1, pp. 19-31, 1996.
[27] J. Bitha and R. V. Solm, "A cycle approach to business continuity planning," *Information Management and Computer Security*, vol. 4, issue 4, pp. 328, 2000.
[28] S. M. Hawkins, D. C. Yen, and D. C. Chou, "Disaster recovery planning: A strategy for data security," *Information Management and Computer Security*, vol. 8, issue 5, pp. 222, 2000.
[29] U. S. Sekaran, *Research Method for Business – A Skill Building Approach*, John Wiley & Sons, 2000.
[30] R. L. Scheaffer, W. Mendenhall III, A. L. Ott, and K.G. Gerow, *Elementary Survey Sampling. 7th Edition*. Brook/ Cole Publishing Company, 2011.

Dr. Nik Zulkarnaen Hj Khidzir, Senior Lecturer has been involved in ICT industry for the past 12 years. He graduated in Computer Science from Universiti Putra Malaysia and obtained his Master's degree (MSc. IT) from UiTM. His research interests are Software Engineering, Information Security Risk Management and Business Computing. He has published several articles in indexed proceedings and journals. He is a member of the IACSIT, IEEE and PECAMP.

Dr. Azlinah Hj. Mohamed, a Prof. and Dean at the Faculty of Computer and Mathematical Sciences, UiTM have been teaching for the past 23 years. Her areas of interest are Artificial Intelligence (AI) and Knowledge Management (KM). She has also co-authored several books, written numerous research articles, and is a regular presenter at international conferences. She is a member of several national and international professional associations and authorities (e.g MITS, WSEAS)

Datin Dr. Noor Habibah Hj. Arshad, an Assoc. Prof. at the Faculty of Computer and Mathematical Sciences, UiTM has been teaching for the past 26 years. Her areas of interest are IT project management, risk management and IT Governance. She has co-authored several books and written numerous academic articles. She is also a reviewer for WSEAS Conference Proceedings and Journal since 2007. She has received several academic awards and research recognition nationally and internationally.

