Success Factors towards Implementation of Business Continuity Management in Organizations

Noorul Halimin Mansol, Najwa Hayaati Mohd Alwi, Waidah Ismail
Islamic Science University of Malaysia

Abstract

In today's Information and Communication Technology (ICT) environment and with current global economics, Business Continuity Management (BCM) becomes a crucial requirement to the organization. BCM is a managerial activity that identifies potential impacts to the organization caused by the threats. However, BCM is only gets the attention when it is demanded by the regulatory compliance or the stakeholders or customers. The implementation of BCM not only involves the information technology (IT) department, but also the business areas that use the IT services. Therefore, this paper aims to explore and identify the success factors on the execution of business continuity management in the organization particularly in Malaysia. In this study, quantitative analysis has been used to explore the organization employee's view and the importance of these factors towards the successful execution of BCM to the organizations.

1. Introduction

BCM is a management process to ensure the continuity of critical process in the organization [1]. Business continuity becomes a high of interest topic to the organization nowadays due to the today's competitive pressures which need the continuous of the business [2]. The development of BCM has been supported by British Standards Institution (BSI), BS 25999. BCM Standards have been produced in two parts which first, BS 25999-1:2006 Business Continuity Management, Code of Practice. The second, BS 25999-2:2007 is Specification for Business Continuity Management which specifies the requirements for implementing, operating and improving a documented BCM System (BCMS) [3].

The development of BCM is a challenge to the organization where it has to keep the organization's management focus on the importance of the business sustainability by considering activities of planning, operational and budgeting [4]. The fundamental of these activities is the involvement of people. It is essential to the organization to adopt and accept BCM not only at certain levels of role for example information technology department, but also the business areas that use the services within the organization [5]. BCM policy and procedures alone cannot ensure the organization's business continuity without some of the external key factors in place. The aim of this paper is to report the results of the exploratory study to identify the success factors which plays a vital role for ensuring the successful of implementation of BCM policy and procedures in the organization.

2. Research Methodology

The results of the research carried out in Malaysian licensed PKI Authority. Three organizations were selected. With the security as the primary concern and been mandated by Malaysian government as the digital certification services provider, these three organization have been selected as the participants for the quantitative study. The participants were represented by different level of roles and department in the organizations. All participants are at senior level with more than five years' experience in their field and generally most of them have a high level of education (graduate level and above).

Close-ended questionnaires were developed for the participants. The questions have been reviewed by three experts from Senior Management level in the organizations and academic institution to ensure the reliability and integrity of the questionnaires. The sessions was arranged and conducted with all the participants at their offices with their convenience. It is important to have secondary information for example documents review such as bulletin, flyers and annual report as the supportive method to the quantitative approach [6]. This will help the researcher to identify what information security incident and management the organization faced and what type of information security awareness program the organization have and communicate to their employees.

3. Research Findings and Discussion

3.1. Management Commitment

Management commitment and support is a vital requirement in order to ensure the successful execution of BCM in the organization. Respondents were asked what is the most factors that might lead to the failure of the execution of BCM. From the results survey that we conducted, 50% of the respondents indicated that lack of management support shall lead to the failure of the execution of BCM in the organization. Generally, the management feels that it is IT department responsibility to maintain the technology use in the organization and keep the organization's information secure [7]. The management will not initiate any measures in order to manage and secure the organization's information. The respondents also indicated that senior management should led the BCM planning and execution in the organization. This confirms what [8], claims that as the prime sponsor and motivator, the senior management should plays their role from the beginning of the execution of BCM.

Information security culture and individual values affects the organizational commitment [9]. The successful of information security cultures in the organization with having top management willingness to provide the resource can contribute the successful of the execution. Therefore, it is essential to set the security behavior at the beginning with those at the top management level [10].

3.2. Awareness

The respondents were asked on the level of priority of the information security in the organization. Most of the respondents' shows their high priority on the information security which to be their main concern. By having information security awareness, they believed that any information security management policy and procedures taken including BCM should be executed successfully in the organization. The results showed that more than half of the numbers of employees indicated that BCM is very important to be in place. Awareness should be adopted in the organization where employees at every level from different department should play their role [11]. The effectiveness of security awareness program is more depending on the behavioral theory requirements and the explanation to the user why they should follow the security procedures or guidelines [12].

3.3. Training and Skills

The study revealed that the most security incidents which the organizations face came from their own users which known as insider threats. This had confirmed Katz study in 2005 [13] which indicated that employee is the biggest threat to information security. Organizations spend millions of dollars on security measures such as encryption, firewalls and secure access devices, but at the end it is still do not address the weakest factor in the security chain which is people [14]. SPAM email had become the most security incidents faced by the participants in the organizations. Viruses were installed when the employee opened the SPAM email where it affected the organization's system.

The study indicated that most of the participants' agree that ongoing education or training shall bring the understanding of the significance and effect of the security threats. Continuous training should be embedded in the organization for employees at all level in the organization. Employees who are the one who going to comply the information security policy mechanism including BCM. It is recommended that BCM training should include the reports of the security incidents faced by the organization. This shall brief the participants the significant of BCM in relations with the security incident. Effort should be put the training program and educate the employees at all level. It is recommended also that the organization to establish a process to evaluate the effectiveness of the training program.

3.4. Information and Knowledge Sharing

Knowledge is the most valuable resource to the organization where all employees in the organization have the knowledge depends on what kind of job they are doing. Information management and knowledge sharing may contribute is the key success where it can contributes the organization competitiveness. Phillip Shupe of Eastman Chemical mentioned that the biggest challenge he face is developing a level of education in the organization is to provide consultancy to all the organizations throughout Eastman Company. Education must start at the top management level. Information system processes for knowledge must be managed securely [15].

BCM is a managerial process to identify potential impact of the business operations in the organization. BCM aim is to produce process and procedures in order to ensure the continuity of the key activities that were affected by disruption or loss [16]. All employees at all level must have necessary knowledge and skills to do their work. Continuous

information transfer is important for the employee to use the knowledge effectively [17]. Beazley et al. [18] indicated that Knowledge continuity management can contribute successful of the knowledge transfer between the employee generations. It is important to have knowledge transfer when the employee leaves the organization or when the organization gets into immediate resignation or critical situation for example a death of an employee.

4. Conclusion

This study has revealed a number of key factors that can be taken by the BCM experts as essential needs to the organization to ensure the level achievement of BCM practice. The study results have suggested that steps must be taken to ensure the continuous BCM training or awareness program to be embed in the organization. By merging BCM program and the exposure of the security threats to the employee, this shall ensure the employees aware of the security threats or issues and the consequence of insecure behavior. Implementation of BCM would not be possible without the management commitment. The organization management should possess a positive behavior and attitudes towards securing the information security in the organization. From the findings, it is expected that it will benefit to the organizations everywhere to have better understanding and identify the steps to improve the implementation of BCM in the organization.

5. References

[1] M. Blyth. (2009) *Business Continuity Management: Building an Effective Incident Management Plan*, Hoboken. NJ:J. Wiley, pp. 362.

[2] Sharjah. (2006) *Information Security and Business Continuity: When Business is Not as Usual!*, KPMG.

[3] K, Roebuck. (2011) *Business Continuity and Disaster Recovery*. UK: Lightning Source UK Ltd.

[4] *Building a Continuity Culture*. (2006), Canada, KPMG LLP.

[5] Paul K., "Integrating Business Continuity Management System into an organization", TechTarget, http://www.searchdisasterrecovery.techtarget.com/tip/Integrating-business-continuity-management-system-into-an-an-organization (12 February 2014).

[6] Klein, K. and Myers, D., (1999), *"A Sets of Principles for Conduction and Evaluating Interpretive Field Studies in Information Systems*. MIS-Quarterly, 23(1): 67-93.

[7] Fung, P. and Jordan, E. (2002), *"Implementation of Information Security: A Knowledge-based Approach*".

[8] Manik, D. (2011) *"Business Continuity Planning (BCP) Methodology – Essential for every business*", 2011 IEEE GCC Conference and Exhibition (GCC), February 19-22, Dubai, United Arab Emirates.

[9] Moon, M. (2000), "*Organizational Commitment Revisited in New Public Management: Motivation, Organizational Culture, Sector, and Managerial level".* Public Performance & Management Review, 24(2): p. 177-194.

[10] Hone, K. & Eloff, J.H.P. (2002), *"What makes an Effective Information Security Policy"*, Network Security, Vol 20, No 6, pp: 14-16.

[11] Andy M. (2009), *"Embbeding BCM In the Organizational's Culture"*, The Business Continuity Journal, Vol. 3, Issue 3, PwC.

[12] Siponen, M. (2000), *"A Conceptual Foundation for Organizational Information Security Awareness"*, Information Management & Computer Security. Vol.8(1): p. 31-41.

[13] Katz, F.H. (2005), *"The Effect of a Univeristy Information Security Survey on Instruction Methods in Information Security.*

[14] Lampson, B. W. (2002), *"Computer Security in the Real World"*, Principles of Computer Systems, www.research.microsoft.com/lampson.

[15] Bouthillier, F., Shearer, K. (2002), *"Understanding Knowledge Management and Information Management: the need of empirical perspective*", Information Research, http://informationR.net/ir/8-1/paper141.html, 8(1).

[16] Stam, CH. (2009), "*Knowledge and the Ageing Employee: A Research Agenda*." INHOLLAND University of Applied Sciences, Haarlem, The Netherlands.

[17] Herbane, B., (2010), "*The evolution of business continuity management: Ahistorical review of practices and drives"*. Business history, Vol.52(6), pp. 978-1002.

[18] Beazley, H., Boenisch, J., Harden, D. (2002), *"Continuity Management:Preserving Corporate Knowledge and Productivity When Employees Leave"* John Wiley & Sons, New York, NY.

