International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:7, 2015

An Investigation on Organisation Cyber Resilience

Arniyati Ahmad, Christopher Johnson, Timothy Storer

***Abstract*—**Cyber exercises used to assess the preparedness of a community against cyber crises, technology failures and Critical Information Infrastructure (CII) incidents. The cyber exercises also called cyber crisis exercise or cyber drill, involved partnerships or collaboration of public and private agencies from several sectors. This study investigates Organisation Cyber Resilience (OCR) of participation sectors in cyber exercise called X Maya in Malaysia. This study used a principal based cyber resilience survey called C-Suite Executive checklist developed by World Economic Forum in 2012. To ensure suitability of the survey to investigate the OCR, the reliability test was conducted on C-Suite Executive checklist items. The research further investigates the differences of OCR in ten Critical National Infrastructure Information (CNII) sectors participated in the cyber exercise. The One Way ANOVA test result showed a statistically significant difference of OCR among ten CNII sectors participated in the cyber exercise.

***Keywords*—**Critical Information Infrastructure, Cyber Resilience, Organisation Cyber Resilience, Reliability Test.

I. Introduction

CRITICAL infrastructures provide services to the community like water supply, electricity, transportation, networks and communications [9]. Any disruption on these infrastructures will affect the social, economy and stability of the whole nation. Therefore, protecting these critical infrastructures is crucial to ensure the continuity of the services to the nation [4]. Critical infrastructures are heavily reliant on cyber space through millions of interconnected computers, information systems and telecommunication networks that support all sectors economy [16], [6]. The part of the information infrastructure that is essential for the continuity of the CI services is known as critical information infrastructure (CII) [6]. The interactions between CII often create complex relationships, dependencies, and interdependencies that cross infrastructure boundaries, rendering the entire system extremely complex and prone to domino failures [16]. As critical infrastructures interact at different levels; failure in one infrastructure may impact the functionality of other infrastructures [9]. For example [4] in 1998, the failure of the Galaxy IV satellite system degraded US telecommunications services, resulting in cascading effects in other infrastructures caused 40 million pagers failed to working. More than twenty United Airlines flights were delayed due to the lack of high altitude weather data. As consequence to the road transportation infrastructure was also affected because highway refueling stations were unable to process credit cards as their satellite links were down. Significantly, any disruptions on critical infrastructures could create a catastrophic damage. It is important to raise awareness of these interdependencies among critical infrastructure owners and operators [12].

Threats to these critical infrastructures fall into two categories [9]: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats").

Major critical infrastructures are owned by private organizations [6]. Partnerships and collaboration between public and private become main agenda of National Critical Infrastructure Protection [1]. One of the efforts is through the cyber exercises to protect the critical infrastructures from cyber threats [7]. Cyber exercises use scenarios to increase the awareness of critical infrastructure operators about interdependencies, threats, vulnerabilities and mitigation policies and procedures [17]. This study investigates organization cyber resilience (OCR) of participation sectors in cyber exercises. To evaluate the usability of the C-Suite Executive checklist survey to assess the Organisation Cyber Resilience (OCR), a reliability test is conducted to assess the internal consistency of the items in the survey. Data for evaluate the C-Suite Executive checklist survey collected using online survey distributed to cyber exercise participants in Malaysia.

This paper is organized into seven sections. The first section explains the background of the study followed by the second section, defines the collaborative cyber exercise. The third section elaborates on cyber resilience. The fourth section describes the research methodology, cyber exercise in Malaysia and data collection. The fifth section explains about data analysis including reliability test and correlation test. The sixth section describes the organisation cyber resilience analysis on ten CNII sectors. The final section concludes with a direction of the future research.

II. Collaboration Cyber Exercise

Generally, cyber exercises as described by [18] have three different purposes: 1) to conduct a cyber-exercise for awareness. This exercise will bring individuals together to make them aware of possible security incidents that their organisation might experience; 2) to use the cyber exercise for education and training. The goal of this training is to prepare the individuals with the response techniques that they may require when deal with security incidents; 3) to test the ability to detect and respond in a coordinated manner in dealing with attack and cyber incidents.

Cyber exercises allow participants to evaluate what-if scenarios and their responses to the events. This can serve as

A. Ahmad is with the University of Glasgow United Kingdom (e-mail: arniyati@gmail.com).

an invaluable awareness tool and business process model evaluation technique [7]. Therefore collaborative cyber exercises are important aspect of public and private cooperation and have been incorporated in cyber strategy in national critical information infrastructure protection as in [12]. This promotes the collaborative cyber exercise used as platforms for situation awareness training, cyber incidents information sharing and cooperation in cyber incidents handling [11].

III. Cyber Resilience

Cyber resilience provides the ability to anticipate, withstand, recover from, and evolve to better address cyber threats [3]. Literatures on cyber resilience have diversity in focus including vocabulary of cyber resilience techniques [2], cyber resilience matrix for cyber systems [13], CERT Resilience management model that focus on managing operational resilience [5] and cyber resilience engineering [3].

This study is focusing on organisation cyber resilience as initiative developed by Economic Forum in 2012. The core principles of the World Economic Forum's Partnering for Cyber Resilience initiative were established to raise awareness of cyber risk and to build commitment regarding the need for more rigorous approaches to cyber risk mitigation. The core principals are [19]: 1) Recognition of interdependence. All parties have a shared interest in fostering a common, resilient digital ecosystem; 2) Role of leadership. Encourage executive-level awareness and leadership of cyber risk management; 3) Integrated risk management. Develop a practical and effective implementation programme that aligns with existing frameworks; 4) Promote uptake. Encourage suppliers and customers alike to develop similar levels of awareness and commitment.

IV. Research Methodology

This study use the C-Suite Executive checklist developed by World Economic Forum in 2012[19] for data collection. Table I shows the list of items in the C-Suite Executive questionnaire contains of 19 questions that cover three main categories [19]: Governance (8 questions), Programme (8 questions) and Network (3 questions). Using 5 ranges of Likert scales defined as 1: Does not describe my organisation at all to 5: Accurately describes my organisation. The average score from all items provides the OCR. In order to ensure the suitability of the tool used to measure the Organisation Cyber Resilience, the reliability test on the C-Suite Executives items conducted in Section V.

A. C-Suite Executive Checklist Survey

TABLE I
C-Suite Executive Survey Items

	C-Suite Executive Checklist Items
	Governance (GV)
GV1	The chief executive and executive management team are responsible for overseeing the development and confirming the implementation of a Programme of best practices for cyber risk management
GV2	The chief executive and executive management team ensure that the Programme is reviewed for effectiveness and, when shortcomings are identified, corrective action is pursued
GV3	The chief executive and the executive management team demonstrate visible and active commitment to the implementation of the Principles
GV4	Executives and managers are responsible for understanding at the appropriate level how cyber risks could impact and originate from their line of business
GV5	Senior leadership understands who is responsible for managing cyber risk when managing security incidents
GV6	The organization has access to cyber expertise at its highest management levels
GV7	The organization undertakes to continuously improve the integration of its cyber risk management with its other risk management initiatives
GV8	The chief executive (or equivalent) has a clear decision path for action and communication in response to a significant security failure or accident
	Programme (PRG)
PRG1	The organization conducts comprehensive assessments of its vulnerabilities to internal and external cyber risks appropriate for its industry and sector
PRG2	The organization monitors the effectiveness of its cyber risk management strategy
PRG3	The organization periodically internally verifies its compliance with rules and regulations
PRG4	The organization's commitment to the Programme is reflected in its policies and practices
PRG5	Managers, employees and agents receive specific training on the Programme, tailored to relevant needs and circumstances
PRG6	The organization has identified its data and information as vital assets, and organizes its Programme around the recognition that data and information have value that can be separately recognized and protected
PRG7	The risk management Programme includes all material third-party relationships and information flows
PRG8	The organization conducts comprehensive internal short- and long-term cyber risk impact assessments
	Network (NTW)
NTW1	The organization seeks to ensure that its suppliers and relevant third parties adhere to the organization's specific cyber risk management standards or industry best practices, in line with the Principles, and formalizes this requirement using contractual obligations
NTW2	The organization has built relationships with its peers and partners to jointly manage cyber risk and more effectively deal with cyber incidents
NTW3	The risk management Programme includes all material third-party relationships and information flows

B. Cyber Exercises in Malaysia

In Malaysia, the Critical Information Infrastructure are defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on Malaysia's national economic strength, economic strength, national image, national defence and security, government capability to function, and public health and safety (National Cyber Security Policy 2006) [1], [8]. With this definition, the NCS policy recognised ten critical sectors which are [1]: national defense and security, banking/finance, information and

communications, energy, transportation, water, health services, government, emergency services, food and agriculture. The NCSP states its objective that Malaysia's Critical National Information Infrastructure (CNII) must be secure and resilient, that is, immune against threats and attacks to its systems [1], [21].

The Malaysia National Security Council with the support of Cyber Security Malaysia organised the collaborative National Cyber Crisis Exercise, known as X-MAYA [10]. This program was conducted to assess the capabilities of CNII agencies to deal with cyber incidents [10] [20]. As shown in Table II, the first cyber exercise was started in 2008 named as X-Maya 1, followed by series of X Maya conducted until the fifth exercise which took place in 2013. The purposes of the National Cyber Crisis Exercise are [10]: 1) To test the effectiveness of Action, Communication and National Security Coordination in dealing with existing cyber crisis; 2) To provide insight into the CNII agencies of government, national defense and security, banking and finance, information and communications, energy, transportation, water, health, emergency services, and agriculture in addressing cyber security incidents, and; 3) To raise awareness about the impact of the crisis on national security in cyberspace among CNII agencies.

TABLE II
CYBER EXERCISES IN MALAYSIA

Cyber Exercise	Year	No of Participants
X-Maya 1	2008	11 Agencies
X-Maya 2	2009	28 Agencies
X-Maya 3	2010	34 Agencies
X-Maya 4	2011	51 Agencies
X-Maya 5	2013	96 Agencies

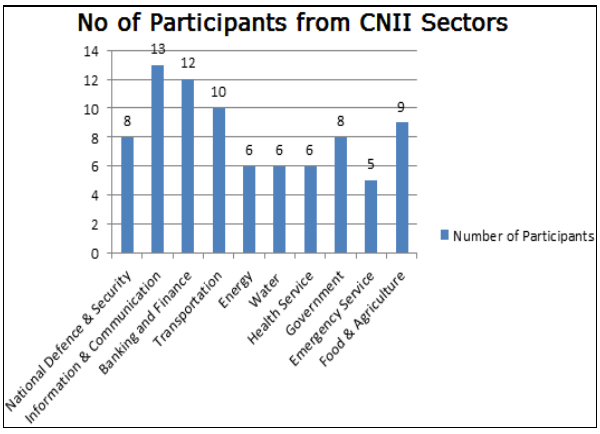

Fig. 1 Survey Participants by Sectors

C. Data Collection

Data for this study collected using online version of C-Suite Executive checklist in [19]. The participants are people that have involved with cyber exercise called X Maya 5 in Malaysia. Participants are contacted by email either direct to them or email through their Sector Leader. Total 83 participants answered the online survey. Fig. 1 shows the number of respondents involved in this study, it showed high frequency of respondents from Information & Communication (13), Banking and Finance (12) and Transportation (10). While same number of respondents are from Energy (6), Water (6) and Health Service (6) sectors.

V. DATA ANALYSIS

A. Reliability Test on C-Suite Executive Checklist

As emphasized by [15], summated scales are often used in survey tools to inquiry underlying constructs that need to be measure. The tools contain set of indexed responses, which are later summed to arrive at a subsequent score associated with a particular respondent [14]. Usually, the development of such scales is not the only aim of the research, but rather a means to collect predictor variables to be use in an objective model. However, the question of reliability increased as the function of scales is strained to include the realm of prediction. One of the most popular reliability statistics uses today is Cronbach's alpha [15]. This study focusing on validates the C-Suite Executive Checklist survey items using the Cronbach's alpha reliability test to check the internal consistency of the items that will be used as a tool to assess the Organisation Cyber Resilience (OCR).

According to [15] the OCR items in C-Suite Executive checklist survey has good internal consistency if the Cronbach's alpha coefficient is more than 0.7. In this study the result of reliability test was very satisfied by Cronbach's alpha coefficient value of 0.974 and 0.975 as described in Table III.

TABLE III
RELIABILITY TEST OF C- SUITE EXECUTIVE CHECKLIST ITEMS

Cronbach's Alpha	**Cronbach's Alpha Based on Standardized Items**	**N of Items**
0.974	0.976	19
0.975	0.977	17

TABLE IV
ITEM TOTAL STATISTICS FOR C- SUITE EXECUTIVE CHECKLIST SURVEY

OCRP Factor	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
GV1	69.5	256.42	0.865	0.972
GV2	69.5	252.45	0.870	0.972
GV3	69.9	250.91	0.778	0.973
GV4	69.6	253.68	0.846	0.972
GV5	69.6	252.54	0.888	0.972
GV6	69.8	254.11	0.807	0.973
GV7	69.5	257.33	0.823	0.973
GV8	69.5	252.06	0.906	0.972
PRG1	69.98	250.98	0.721	0.974
PRG2	69.94	250.98	0.767	0.973
PRG3	69.47	256.50	0.824	0.973
PRG4	69.53	252.64	0.897	0.972
PRG5	69.93	256.56	**0.682**	0.974
PRG6	69.73	253.72	0.905	0.972
PRG7	69.96	253.13	0.721	0.974
PRG8	69.96	253.91	**0.689**	0.974
NTW1	69.59	253.81	0.853	0.972
NTW2	69.63	256.60	0.811	0.973
NTW3	69.65	252.96	0.817	0.972

All items achieved Corrected Item-Total correlation ranging

from 0.682 to 0.906. As suggested by [14] that items which have low score which is less than 0.7 which indicates that the items are measuring something different from the scale as a whole [15]. As in Table IV, items PRG5 and PRG8 showed Corrected Item-Total of 0.682 and 0.689 which below than 0.7. Removing the items from the set showed a small difference in score of 0.001(0.975-0.974) as shown in Table IV, with the minimal effect, for that reason both items will not be removed from the original set.

B. Descriptive Analysis

Table V shows the descriptive analysis of C-Suite Executive three main components of governance, programme and network.

TABLE V
DESCRIPTIVE ANALYSIS OF GOVERNANCE, PROGRAMME AND NETWORK

	N	Mean	Standard Deviation
OCR	83	3.872	0.884
AvgGV	83	3.964	0.916
AvgPRG	83	3.753	0.961
AvgNTW	83	3.944	0.961

C. Pearson Correlation Test

The Pearson's product moment coefficient of correlation, is one of the best-known measures of association, it is a statistical value ranging from -1.0 to +1.0 to express the relationship in quantitative form [14]. The coefficient is represented by the symbol r. The Pearson correlation test was conducted to see the relationship between dependent variable (OCR) with independent variables governance (AvgGV), programme (AvgPRG) and network (AvgNTW).

TABLE VI
PEARSON CORRELATION TEST OF C- SUITE EXECUTIVE CHECKLIST

OCR	AvgGV	AvgPRG	AvgNTW
Pearson Correlation (r)	0.965**	0.931**	0.895**
Sig. (2- tailed)	0.000	0.000	0.000
N	83	83	83

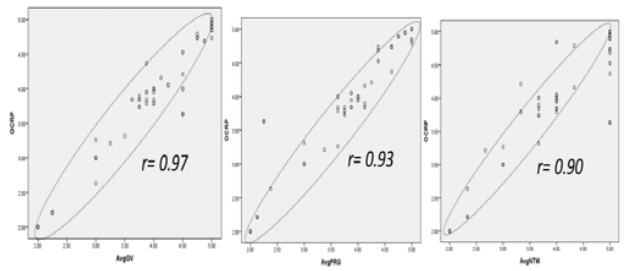

Fig. 2 OCR Correlation Scatterplots

Table VI and correlation scatterplots in Fig. 2 show the high positive correlation between AvgGV and OCR with r=0.97, AvgPRG and OCR with r=0.93 and AvgNTW with OCR with r=0.90. This indicates that the increment of governance, programme and network factors will strongly influence the OCR.

VI. ORGANISATION CYBER RESILIENCE STUDY ON CNII SECTORS

A. Descriptive Analysis

Further investigation conducted to test the OCR differences for multiple sectors involved in the cyber exercise. A one way between-group analysis of variance conducted to see if there were any differences on Organisation Cyber Resilience (OCR) between ten CNII sectors participated in the X Maya 5 cyber exercise. The OCR of ten CNII sectors are described in Table VII.

TABLE VII
DESCRIPTIVE ANALYSIS OF TEN CNII SECTORS

Sectors	N	Mean (OCR)	Standard Deviation
National Defence & Security	8	4.086	0.603
Energy	6	4.509	0.554
Banking & Finance	12	4.640	0.358
Information & Communication	13	4.486	0.473
Transportation	10	3.321	0.538
Water	6	2.798	0.767
Health Services	6	3.149	0.884
Government	8	4.224	0.441
Emergency Service	5	3.116	0.935
Food & Agriculture	9	3.263	0.908

B. A One Way Anova Test

A one-way between-group analysis of variance was conducted to explore the organisation cyber resilience group of ten CNII sectors participated in cyber exercise with the hypothesis stated below:

- *H0: There is no statistically significant difference on organisation cyber resilience (OCR) between CNII sectors participated in collaborative cyber exercise.*
- *Ha: There is a statistically significant difference of organization cyber resilience (OCR) between CNII sectors participated in collaborative cyber exercise.*

TABLE VIII
ANOVA TEST RESULT

OCR	Sum of Squares	df	Mean Square	F	Sig
Between Groups	35.054	9	3.895	9.779	0.000
Within Groups	29.075	73	0.398		
Total	64.128	82			

The test result in Table VIII shows that there were statistically significant differences in Organisation Cyber Resilience (OCR) between ten CNII sectors at the $p < 0.05$ level. Despite reaching statistical significance, the actual difference in mean scores between group was medium effect based on effect size calculated using eta squared was 0.6. Details of multiple comparisons between sectors shows in Table IX, the Post Hoc test results displays how one sector was difference from other sectors. These also indicated that the mean score (OCR) was medium for three different groups: Group 1 (energy, banking & finance, Information & Communication), Group 2 (Government and National Defence & Security) and Group 3 (Transportation, Water, Health Services, Food & Agriculture and Emergency Service.

TABLE IX
POST HOC TEST RESULTS

Comparison OCR between Sectors		Mean Differ.	Std. Err.	Sig.	Hypothesis *p<0.05 reject H0*
National Defence & Security (Group 1)	Water	1.287*	0.341	0.01	*reject H0*
Energy (Group 2)	Transportation	1.188*	0.326	0.02	*reject H0*
	Water	1.711*	0.364	0.00	*reject H0*
	Health Services	1.360*	0.364	0.01	*reject H0*
	Emergency Service	1.393*	0.382	0.02	*reject H0*
	Food & Agriculture	1.246*	0.333	0.01	*reject H0*
Banking & Finance (Group 3)	Transportation	1.319*	0.270	0.00	*reject H0*
	Water	1.842*	0.316	0.00	*reject H0*
	Health Services	1.491*	0.316	0.00	*reject H0*
	Emergency Service	1.525*	0.336	0.00	*reject H0*
	Food & Agriculture	1.377*	0.278	0.00	*reject H0*
Information & Communication (Group 4)	Transportation	1.165*	0.265	0.00	*reject H0*
	Water	1.688*	0.311	0.00	*reject H0*
	Health Services	1.337*	0.311	0.00	*reject H0*
	Emergency Service	1.370*	0.332	0.00	*reject H0*
	Food & Agriculture	1.222*	0.274	0.00	*reject H0*
Transportation (Group 5)	Energy	-1.188*	0.326	0.02	*reject H0*
	Banking & Finance	-1.319*	0.270	0.00	*reject H0*
	Information & Communication	-1.165*	0.265	0.00	*reject H0*
Water (Group 6)	National Defence & Security	-1.287*	0.341	0.01	*reject H0*
	Energy	-1.711*	0.364	0.00	*reject H0*
	Banking & Finance	-1.842*	0.316	0.00	*reject H0*
	Government	-1.425*	0.341	0.00	*reject H0*
Health Services (Group 7)	Energy	-1.359*	0.364	0.01	*reject H0*
	Banking & Finance	-1.491*	0.316	0.00	*reject H0*
	Information & Communication	-1.34*	0.311	0.00	*reject H0*
Government (Group 8)	Water	1.425*	0.341	0.00	*reject H0*
Emergency Service (Group 9)	Energy	-1.393*	0.382	0.02	*reject H0*
	Banking & Finance	-1.525*	0.336	0.00	*reject H0*
	Information & Communication	-1.370*	0.332	0.00	*reject H0*
Food & Agriculture (Group 10)	Energy	-1.246*	0.333	0.01	*reject H0*
	Banking & Finance	-1.377*	0.278	0.00	*reject H0*
	Information & Communication	-1.222*	0.274	0.00	*reject H0*

VII. CONCLUSION AND FUTURE WORK

The Cronbach's Alpha test conducted on 19 items of C-Suite Executive checklist survey showed a good internal consistency of 0.974. The Pearson correlation test on OCR components showed a very high positive relationship between OCR with governance, programme and network components with Pearson coefficient value ranging from 0.90 to 0.97. This suggests that the increment of these components will increase the OCR of participated sectors. This also indicated the appropriateness use of the C-Suite Executive checklist survey to assess the OCR in a future study. The future study will be continued to test the relationship of collaborative cyber exercise with OCR. This will involve a comparison between sectors with collaborative cyber exercises experiences with sectors without cyber exercises experiences.

ACKNOWLEDGMENT

This study has granted the right to use the C-Suite Executive checklist Survey from World Economic Forum Committee in 2013.

REFERENCES

[1] Hashim, M. S. Malaysia's National Cyber Security Policy
[2] Bodeau, D., & Graubart, R. (2013, November). Intended effects of cyber resiliency techniques on adversary activities. In Technologies for Homeland Security (HST), 2013 IEEE International Conference on (pp. 7-11). IEEE.
[3] Bodeau, D., & Graubart, R. (2011). Cyber Resiliency Engineering Framework.
[4] Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. Journal of Contingencies and Crisis Management, 15(1), 50-59
[5] Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2010, August). Improving Operational Resilience Processes: The CERT Resilience Management Model. In Social Computing (SocialCom), 2010 IEEE Second International Conference on (pp. 1165-1170). IEEE.
[6] Cavelty, M. D. (2007). Critical information infrastructure: vulnerabilities, threats and responses. In Disarmament Forum (Vol. 3, pp. 15-22).
[7] Conklin, A., & White, G. B. (2006, January). E-government and cyber security: the role of cyber security exercises. In System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on (Vol. 4, pp. 79b-79b). IEEE.
[8] Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. Government Information Quarterly, 26(4), 584-593.

[9] Glorioso, A., & Servida, A. (2012). Infrastructure sectors and the information infrastructure. In Critical Infrastructure Protection (pp. 39-51). Springer Berlin Heidelberg.
[10] Government Launches National Cyber Crisis Management Policy and Mechanism, http://vsdaily.com/tag/x-maya-5/.Accessed January 18, 2013).
[11] Hernantes, J., Lauge, A., Labaka, L., Rich, E., Sveen, F. O., Sarriegi, J. M., & Gonzalez, J. J. (2011, January). Collaborative modeling of awareness in Critical Infrastructure Protection. In System Sciences (HICSS), 2011 44th Hawaii International Conference on (pp. 1-10). IEEE.
[12] Kwak, Y. H., Chih, Y., & Ibbs, C. W. (2009). Towards a comprehensive understanding of public private partnerships for infrastructure development. California Management Review, 51(2), 51-78.
[13] Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471-476.
[14] Pallant, J. (2013). SPSS survival manual. McGraw-Hill International.
[15] Santos, J. R. A. (1999). Cronbach's alpha: A tool for assessing the reliability of scales. Journal of extension, 37(2), 1-5.
[16] Setola, R., De Porcellinis, S., & Sforna, M. (2009). Critical infrastructure dependency assessment using the input–output inoperability model. International Journal of Critical Infrastructure Protection, 2(4), 170-178.
[17] Solansky, S. T., & Beck, T. E. (2009). Enhancing community safety and security through understanding interagency collaboration in cyber-terrorism exercises. Administration & Society, 40(8), 852-875.
[18] White, G. B., Dietrich, G., & Goles, T. (2004, January). Cyber security exercises: testing an organization's ability to prevent, detect, and respond to cyber security events. In System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on (pp. 10-pp). IEEE.
[19] World Economic Forum, Partnering for Cyber Resilience, Risk and Responsibility in a Hyper connected World, March 2012
[20] X Maya 3: Benchmarking the National Cyber Crisis Management Plan. http://www.cybersecurity.my/en/knowledge_bank/news/2010/main/detail/1906/index.htm. (Accessed in February 12, 2013).
[21] Yunos, Z., Hafidz Suid, S., Ahmad, R., & Ismail, Z. (2010, August). Safeguarding Malaysia's critical national information infrastructure (CNII) against cyber terrorism: Towards development of a policy framework. In Information Assurance and Security (IAS), 2010 Sixth International Conference on (pp. 21-27). IEEE.