Cyber Security Defence Policies: A Proposed Guidelines for Organisations Cyber Security Practices

Julius Olusegun Oyelami[1], Azleena Mohd Kassim[2]
School of Computer Sciences
Universiti Sains Malaysia
Penang, Malaysia

***Abstract*—Many organisations have been struggling to defend their cyberspace without a specific direction or guidelines to follow and they have described and identified cyber attack as a devastating potential on business operation in a broader perspective. Since then, researchers in cyber security have come out with numerous reports on threats and attack on organisations. This study is conducted to develop and propose a Cyber Security Defence Policies (CSDP) by harmonising and synthesizing the existing practices identified from the literature review. Observation and questionnaire were adopted to evaluate, review and collect data under ethical agreement from 10 organisations. The validation is based on the principal components for the proposed CSDP and the proposed CSDP, using SPSS as the statistical tool. The result shows that, the validation of the proposed CSDP by 20 experts reveals a standard deviation of 0.607, 0.759, 0.801, 0.754, 0.513, 0.587 and 0.510 on each of the principal components without a missing value respectively. While the correlation matrix and the reproduced correlation matrix for the proposed CSDP indicated 61% and the percentage of acceptance on the principal components for the proposed CSDP are higher than 50%. Therefore, from the outcome, it has shown that the acceptance responds towards the proposed CSDP and the result from the principal components analysis (eigenvalue analysis) are significant enough for implementation and can be adopted by organisations as a guidelines for organisation cyber security practices.**

Keywords—Cyber security; cyber defence policy; organisation; cyber security practices

I. Introduction

Many organisations have described and identified cyber attack as potentially having some devastating implications on business operation in a broader perspective. Thus, researchers in security have come out with numerous reports on threats and attack on organisations [1]. Cyber security weaknesses have been widespread, taking place on organisation and pose risk on their assets [2]. Many organisations have been struggling to defend their cyberspace without a specific direction or guidelines to follow. Recent studies have shown that, implementation of cloud security (CSe) is a measure that could be used as a security policy [3], [4]. This reasoning is supported by [1], where they stated that in implementing CSe, organisation need to evaluate IT resource with its management portfolio, aligned with the organisation’s strategies and objectives to establish logical security system control to verify the confidentiality, integrity, and availability of information.

Deficiencies in organisation’s cyber security implementation and policy are becoming a global issue and more challenging where it has raised growing concern among professional [6], [7]. Over the years there has been series of cyber-attack reports on organizations asset which has been noted as high-risk area to many organisations as most attacks are from the network system [4], [5], [11]. The emergence of the networking security standard like(i.e., IEEE 802.11, ISO27001 has therefore contributed to the network and cyber security but its deployment in many organisations are still few and organisation need more harmonise standards to combat cyber attacks [9], [10]. Many organisations are going into cloud without observing the threats involved [3]. While wireless network provides opportunity for greater mobility and flexibility for organisation operations, it also poses security risks to the organisation at large [2], [5], [9]. It is recommended for organisations to combine management and technical controls [7], [11], [14]. A report by [12] submitted that more cyber-attacks are expected by the fall of 2020. In line with that, a fully-owned subsidiary of Intel Corporation have also indicated that cyber-crimes are causing the global economy to lose more than $400 billion every year according to report from [4] and [13]. Cyber security involves something more than just a passive compliance with security practices. Cyber-crime and cyber-attack today is becoming inevitable to many organisation, both in government and private sector, and the best way to maintain cyber security is to implement a proactive approach towards virtual security at all times [5], [7], [11].

In this paper, we intend to identify policies which organisations can implement as security policies for cyberspace. Therefore, in this paper, it is postulated that these identified policies can be used as a blueprint for organisation cyber security practices. Our objectives in this paper are to identify several security program practice by these organisations and synchronise the identified security practices into one holistic framework for cyber security defence policies.

The gap analysis from the literature review had suggested that many organisations are still struggling to identify effective cyber security policies for information and data protection without knowing the right security policies to implement. Thus, the proposed cyber security defense policies can be useful for cyber security application.

The next section in this paper will present the related works that have been done in cyber security disaster recovery (CSDR), cyber security governance (CSG), cyber security risk management (CSRM), cyber security incident monitoring and auditing (CSIMA), cyber security intelligent objectives (CSIO), could security (CSe) and cyber security management program (CSMP). Next, the methodology of this study is presented, followed by validating the proposed Cyber Security Defence Policies (CSDP). The proposed blueprint is presented followed by discussions and the future directions as the continuation from this paper are also presented.

II. Related Works

In [7], the cyber security is used as one of the measures that an organisation could take to mitigate cyber-attack, and this argument is further supported by [5]. Mittal [5] stated that an organisation needs to implement cyber security disaster recovery (CSDR) in respect to cyber security, which might enable the organisation to evaluate abilities to continue business operations in the case of cyber incidents. Studies have also shown that cyber security governance (CSG) play an important role in security policy making [1], [7], [8]. In a similar fashion, [4] has shown that organisations need cyber security intelligent objectives (CSIO) to withstand the challenges of security breaches and this statement is credited to the report made by National Institute of Standard and Technology [4]. They further argue that, for organisation to implement CSIO, they need periodical review of cyber security systems and information technology architecture and also perform technical security testing to identify potential threats and vulnerabilities. Mittal [5] agreed with the statement put forward by [6] that organisation's information technology practices need to be aligned with other security practices to ensure effective cyber security intelligence.

According to [6] and [8], in order to identify potential threats, organisations need to evaluate their existing IT policies, practices and data governance to ensure compliance with regulatory and legal requirements as to improve the quality and control of the organisation cyberspace. Studies by [3] and [4] presented cyber security risk management (CSRM) which was identified as one the practices required in organisation to manage risk associated with cyber attacks. They further argued that, organisations need to evaluate data classification practices for adequate alignment with the organization's policies and evaluate the information security and privacy policies practices to ensure that the physical and environmental controls of information assets are adequately safeguarded. As indicated in [2] and [5], the use of cyber security management program (CSMP) is important to outline cyber security policies and practices which will relate to the organisation's knowledge management life-cycle and cyber security life-cycle management in order to select supplier, manage project policies and practices that involve system review (software projects).

In [7], it was stated that, to determine whether project requirements are met before implementation and also to check every phases of project for bugs and other malicious elements in the system development life-cycle, a security management program is required. This could be a move to mitigate security breaches. In a similar fashion, studies conducted by [6] and [9] expressed a concern that, organisation need to perform cyber security audit and monitor incidents in accordance with audit standards and a risk-based audit strategy and it will enable organisation to establish whether systems are protected to provide value to the organisation.

In [10], the cyber security incident monitoring and auditing (CSIMA) was claimed to be able to report and document all activities in the context of cyber security decision making, evaluate whether the risks have been sufficiently addressed and create confidence report to stakeholders. If security practices are harmonised, it could create a strong defensive mechanism in the cyberspace [9], [10], [11]. It was asserted that, people around the world will communicate and exchange information and ideas irrespective of physical location or geographical distances [5], [9], [11]. Today, the cyber world has transformed our lives and makes that possible [7], [14]. As our lives are revolving around the internet of thing (IoT), all our activities also seem to depend on it. Organisation should be aware of their current situation and know how to build a comprehensive cyber security policy. Upon weighing the organisation's susceptibility to risk, along with mitigation and assessment of their current practices, if the organisation is able to observe a gap that could be vulnerable to attacks; then, urgent action is highly recommended to consolidate, integrate and build a formidable mitigation plan.

The works by [15], [16], [17] and [18] agreed that a single security standard, security policy and security practice is not enough to combat cyber terrorism and cyber criminals due to the advancement in technology. These studies agreed that cyber crimes are transnational crimes that are affecting both organisations and humanity. Therefore, in this era, organisations need to harmonise security frameworks security standards and security practices to stand the new challenges emanating from cyber crime.

III. Validating the Proposed Cyber Security Defence Policies (CSDP)

In this study, a preliminary investigation using survey questionnaires was deployed to identify security practices of these 10 organisations both in Africa and Asia. The preliminary investigation was based on cyber security practices of these organisations as this study intend not to reveal the names and identity of these organisations base on the agreed ethic for data collection.

As shown in Table I, organisations labelled as 1, 2, 4, 5, and 7 observe security practices CSe, CSIO CSDR, CSG, CSRM and CSMP respectively. It was also identified that, organisation 3, 6, 8, 9 and 10 practice combination of at least two different practices. CSIMA was practiced in organisations labelled as 8 and 9, both combined with two different practices; the first combined with CSe and the latter combined with CSG. These practices (i.e., CSe, CSIO, CSDR, CSG, CSRM, CSMP, and CSIMA) are harmonized as a component to formulate and propose the Cyber Security Defence Policies (CSDP); in order to accommodate the difference practices.

TABLE I. SUMMARY OF THE ORGANISATION IDENTIFIED SECURITY PRACTICES

Organisation Number	Identified Practices	Abbreviation
1	Cloud Security	CSe
2	Cyber Security Intelligent Objectives	CSIO
3	Cyber Security Intelligent Objectives & Cyber Security Governance	CSIO, CSG
4	Cyber Security Disaster Recovery	CSDR
5	Cyber Security Governance	CSG
6	Cyber Security Risk Management & Cyber Security Disaster Recovery	CSRM, CSDR
7	Cyber Security Management Program	CSMP
8	Cyber Security Incident Monitoring and Auditing & Cloud Security	CSIMA, CSe
9	Cyber Security Incident Monitoring And Auditing & Cyber Security Governance	CSIMA, CSG
10	Cyber Security Risk Management and Cyber Security Governance & Cyber Security Governance	CSRM, CSG

A. *About the Organisations*

These ten organisations are both private and government organisations. The government organisations were established more than a decade ago while the private organisations were established not less than six years. These organisations have been identified as having good reputations for cyber security programs based on the result from the investigation and they have successfully configured applicable security management policies in-place. Each of these policies outlined specific examples on techniques and control used by these organisations to increase their security program's effectiveness.

B. *Validating Procedure*

In this work, the seven security practices are benchmarked and organised under several technical practices identified from the preliminary investigation conducted on 10 organisations from two continents, specifically in Malaysia and Nigeria. We validated these practices using 20 experts from the cyber security area and information security discipline. The experts are in a positions of Information Security Officer’s (ISO), Information Technology Manager’s (ITM) and Chief Information Officer’s (CIO). We selected our independent and dependent variables and the scale of measurements was adjusted to 0.05, where value that is less than 0.05 will indicate rejection and value more than 0.05 will indicate acceptance.

The variables and scaling sampling takes account of exact values from variables such as age, gender, job title and years of work experience. Some variables are assigned with weights to indicate the different level of importance of the respective variables’ values, such as; Level of certification in Information Technology i.e. Basic=5, Intermediate=10 and Expert=15, Level of education i.e. Diploma=5, B.Sc=10, MSc=15 and PhD=20, Area of Expertise i.e. Information security=1, Information security management=2, and Cyber security =3.

The validation is based on (1) the proposed Cyber Security Defence Policy (CSDP) and (2) the principal components (i.e. content analysis) observed from the 10 organisations. Data was collected using questionnaire and the design of the questionnaires were based on the security practices identified from both the literature review and the identified security practices during preliminary investigation using survey questionnaire as a component in formulating the proposed CSDP.

C. *Statistical Procedure*

Initially, this study carry out most of the descriptive statistics concerning the variables assessed using Likert scale. Our test focus on standard multiple regression and linear regression using Statistical Package for Social Science (SPSS). Subsequently, this study proceeds to determine each of the components within the Cyber Security Defence Policies (CSDP) using factor analysis and eigenvalue analysis. This eigenvalue analysis is a linear operation that will provide the properties of the CSDP structure. Reliability on the security practices was determined using Cronbach’s alpha coefficient. The questionnaire focused on the identified practices for the content analysis for the proposed CSDP. Likert scaling was deployed to anchor the responses and to enable the respondents to read meaning to the questionnaires (Strongly agree=5, Agree=4, Neutral=3, Disagree=2, and Strongly disagree=1). The ANOVA experiment was considered by using SPSS statistical analytical tool using descriptive methods and to established correlation between the total score using factor analysis and the results are presented in tables and graph for visualization. In our test for regression analysis, scale of measurement between 0.35 and 0.50 was used as an average value.

D. *Data Analysis*

In the data analysis, as shown in Table II and Table III, where they depict the descriptive analysis on the propose Cyber Security Defence Policies (CSDP) and the total variance of the CSDP on the seven components for the proposed CSDP. Where as Table IV and Table V illustrate the correlation matrix and the reproduced correlation matrix on the seven CSDP components for the propose CSDP. Based on the validation of the proposed CSDP by 20 experts, the descriptive analysis reveals a standard deviation of 0.607, 0.759, 0.801, 0.754, 0.513, 0.587 and 0.510 on each of the seven principal component without a missing value respectively, as illustrated in Table II.

This indicates that, the seven principal component for the proposed CSDP are reliable to be implemented. In calculating the matrix of correlation between items, we excluded value lower than 0.25. For example, the value between 0.09 and 0.24 are considered as a small value, while value between 0.35 and 0.50 can be considered as an average value in this study. While conducting the analysis to explore the setting of our questionnaires based on the seven principal components, it allows us to check each of our parameters on a set of variables obtained. The results point to the extraction of minimum of 25% and maximum of 50% with a total percentile of 75% as shown in Table II. Fig. 1 depicts the scree plot for the eigenvalue analysis, which shows the line plot of the eigenvalue of factors or the principal components in an analysis. Since we retained seven factors as components for the proposed CSDP, this eigenvalue analysis provides the properties of the CSDP as a structure and represent the value for each components. This shows that the proposed CSDP based on its seven components, increased in value with 2.4. This indicate that the proposed CSDP can be brought forward as a guideline in cyber security practices in organisation.

Fig. 2 illustrates the percentage of acceptance based on the seven components. Fig. 2 explains the result from the validation of the proposed CSDP by security experts, and it also illustrates the acceptance rate of each of the principal components for the proposed CSDP (CSe 46%, CSIO 60%, CSDR 65%, CSG 60%, CSRM 60%, CSMP 62% and CSIMA 69%) The correlation matrix and the reproduced correlation matrix are shown in Table IV and Table V for the proposed CSDP, indicate 61% with an absolute values greater than 0.05. This means that from the factors analysis based on the ANOVA test results on the seven components for the proposed CSDP by the experts has shown that, the acceptance respond towards the proposed CSDP are significant enough for implementation and can be adopted by organisations as a blueprint for organisation cyber security policies.

TABLE II. THE DESCRIPTIVE ANALYSIS ON CYBER SECURITY DEFENCE POLICY (CSDP)

		CSe	CSIO	CSDRP	CSG	CSRM	CSMP	CSIMA
N	***Valid***	20	20	20	20	20	20	20
	Missing	0	0	0	0	0	0	0
Std. Deviation		.607	.759	.801	.754	.513	.587	.510
Variance		.368	.576	.642	.568	.263	.345	.261
Minimum		3	3	3	3	4	3	4
Maximum		5	5	5	5	5	5	5
Percentiles	***25***	4.00	4.00	4.00	4.00	4.00	4.00	4.00
	50	5.00	5.00	4.50	5.00	4.50	4.00	5.00
	75	5.00	5.00	5.00	5.00	5.00	5.00	5.00

TABLE III. THE TOTAL VARIANCE OF THE CSDP PRINCIPAL COMPONENTS

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	*% of Variance*	*Cumulative %*	*Total*	*% of Variance*	*Cumulative %*
1	2.308	32.970	32.970	2.308	32.970	32.970
2	1.623	23.185	56.155	1.623	23.185	56.155
3	1.286	18.376	74.531	1.286	18.376	74.531
4	.716	10.231	84.762			
5	.520	7.423	92.185			
6	.358	5.110	97.296			
7	.189	2.704	100.000			

Extraction Method: Principal Component Analysis.

TABLE IV. THE CORRELATION MATRIX ON THE CSDP COMPONENTS

		CSe	CSIO	CSDRP	CSG	CSRM	CSMP	CSIMA
Correlation	**CSe**	1.000	.057	.216	.230	.169	.074	.425
	CSIO	.057	1.000	.459	.221	-.203	.455	.143
	CSDRP	.216	.459	1.000	.401	-.256	.324	.090
	CSG	.230	.221	.401	1.000	.272	-.095	.082
	CSRM	.169	-.203	-.256	.272	1.000	-.437	.101
	CSMP	.074	.455	.324	-.095	-.437	1.000	.553
	CSIMA	.425	.143	.090	.082	.101	.553	1.000
Sig. (1-tailed)	**CSe**		.405	.180	.165	.238	.379	.031
	CSIO	.405		.021	.175	.196	.022	.274
	CSDRP	.180	.021		.040	.138	.081	.353
	CSG	.165	.175	.040		.123	.345	.365
	CSRM	.238	.196	.138	.123		.027	.337
	CSMP	.379	.022	.081	.345	.027		.006
	CSIMA	.031	.274	.353	.365	.337	.006	

TABLE V. THE REPRODUCED CORRELATION MATRIX ON THE CSDP COMPONENTS

		C.Se	CSIO	CSDRP	CSG	CSRM	CSMP	CSIMA
Reproduced Correlation[a]	C.Se	.615[a]	.100	.165	.360	.362	.179	.600
	CSIO	.100	.617[a]	.651	.304	-.373	.488	.152
	CSDRP	.165	.651	.750[a]	.517	-.243	.361	.091
	CSG	.360	.304	.517	.784[a]	.343	-.173	.013
	CSRM	.362	-.373	-.243	.343	.723[a]	-.527	.079
	CSMP	.179	.488	.361	-.173	-.527	.860[a]	.572
	CSIMA	.600	.152	.091	.013	.079	.572	.867[a]
Residual[b]	C.Se		-.043	.052	-.130	-.193	-.105	-.176
	CSIO	-.043		-.192	-.084	.170	-.033	-.010
	CSDRP	.052	-.192		-.117	-.013	-.037	-.001
	CSG	-.130	-.084	-.117		-.071	.077	.069
	CSRM	-.193	.170	-.013	-.071		.090	.022
	CSMP	-.105	-.033	-.037	.077	.090		-.019
	CSIMA	-.176	-.010	-.001	.069	.022	-.019	

Extraction Method: Principal Component Analysis.

a. Reproduced communalities

b. Residuals are computed between observed and reproduced correlations. There are 13 (61.0%) non redundant residuals with absolute values greater than 0.05.

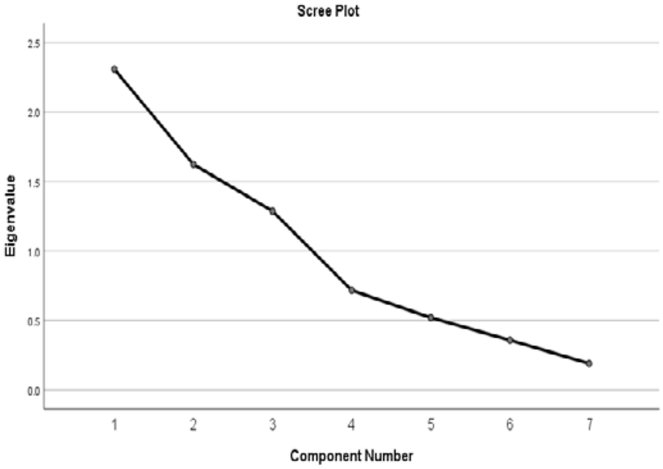

Fig. 1. Scree Plot for the Eigenvalue Analysis (Principal Components Analysis) for the Proposed CSDP.

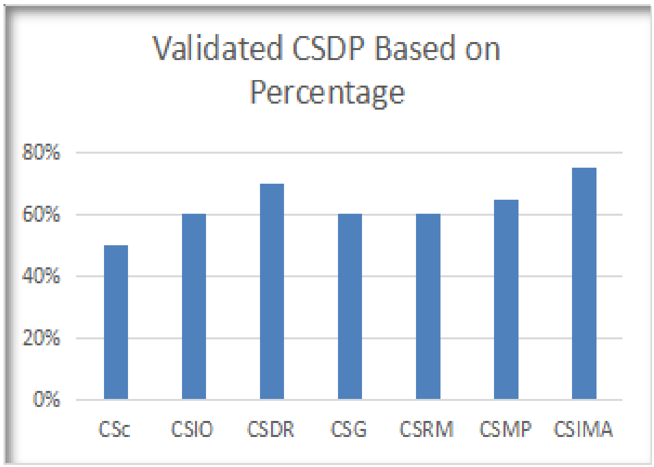

Fig. 2. The Validated CSDP based on Percentage of Acceptance.

IV. RESULT

Based on the data analysis and the validation of the proposed Cyber Security Defence Policies (CSDP) by 20 experts, the descriptive analysis reveals a standard deviation of 0.607, 0.759, 0.801, 0.754, 0.513, 0.587 and 0.510 on each of the principal component without a missing value, respectively, as illustrated in Table I. It indicates that the seven principal component for the (CSDP) are reliable for implementation. In order to calculate the matrix of correlation between items, value lower than 0.25 were excluded. We used the value of 0.09 and 0.24 can be considered as a small value, while value between 0.35 and 0.50 can be considered as an average and the value between the 0.50 and 2 can be interpreted to be a big or large value, therefore, we eliminate all indicators with a correlation less than 0.35.

While conducting analysis to explore the setting of our questionnaires based on the seven principal components analysis, we are able to check each of our parameters on a set of variables obtained. The results point to the extraction of three factors with about 75% of the total variance as shown in Table I. Fig. 1 depicts the screen plot that corroborates this analysis and Fig. 2 illustrates the percentage of acceptance. The correlation matrix and the reproduced correlation matrix are shown in Table III and Table IV.

For the proposed CSDP, it indicates 61% with an absolute values greater than 0.05. Based on the factors analysis, the ANOVA test results on the proposed CSDP and the principal components (eigenvalue analysis) of the CSDP by the experts, the acceptance responds towards the proposed CSDP and its principal components are significant enough for implementation and can be adopted by organisations as a blueprint for organisation cyber security practices. In this study, finding shows that 1) not all organisations are practicing most of the identified security practices, 2) these organisations implemented specific practices according to their need while neglecting other aspect of security measures, 3) the formulated

CSDP might be more effective than the existing security practices due to its completeness with other security practices identified from other organisations, 4) the proposed CSDP might be a complete and harmonised security practices that can support the entire security operations and defend the organisations from cyber criminals and cyber attacks against valuable assets (i.e., information, data and intellectual properties) and 5) implementing CSDP will cover a wide range of security management and create insight on how organisations should create an effective security policies to guide security practices.

V. Discussion

This paper presents the proposed Cyber Security Defence Policies (CSDP) that could be used by any organisation as a blueprint to follow and to guide to secure data and information. This CSDP is recommended for: 1) organisations that intend to plan, develop, implement cyber security policies, 2) individuals or information technology professional i.e. computer system and network engineer, who design, deploy, administer and maintain organisation network security systems, 3) individuals/IT professional who are information security or network security personnel with information system, monitoring responsibilities on organisational information security management, 4) management personnel who might require a technical basis for supporting a decision-making process and 5) those wishing to increase their knowledge on cyber security policies as well.

Fig. 3 illustrates the proposed CSDP as a guideline for organisation to follow when implementing cyber security practices. Organisation that intends to implement Cyber Security Defence Policies (CSDP) should identify the seven basic components within the proposed CSDP. This involves the implementation of Cloud Security (CSe). Cloud security enables organisation to check on IT vendors' products properly before implementing the product to avoid security risk, and it also allows the organisation to secure their data in the cloud as well as create opportunity for organisation to identify risk of mistaken identity during and after implementing authentication platform for data and information users. Data in the cloud need encryption standards and procedures mechanism. With the implementation of CSDP, the organisation will have the advantage to detect the threats that posed a great danger to organisation infrastructure and enhance identity and access management control.

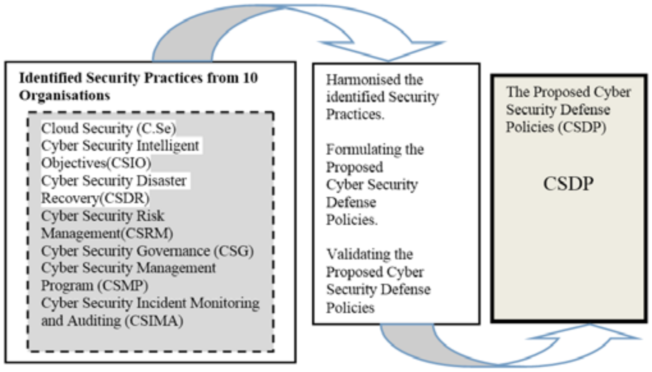
Identified Security Practices from 10 Organisations
Cloud Security (C.Se)
Cyber Security Intelligent Objectives(CSIO)
Cyber Security Disaster Recovery(CSDR)
Cyber Security Risk Management(CSRM)
Cyber Security Governance (CSG)
Cyber Security Management Program (CSMP)
Cyber Security Incident Monitoring and Auditing (CSIMA)
Harmonised the identified Security Practices.
Formulating the Proposed Cyber Security Defense Policies.
Validating the Proposed Cyber Security Defense Policies
The Proposed Cyber Security Defense Policies (CSDP)
CSDP

Fig. 3. The Proposed Cyber Security Defence Policies (CSDP).

The implementation of CSDP will enhance Cyber Security Intelligent Objectives (CSIO) for the organisation by improving the role base access control. This enables the organisation to access role and monitor duty that are performed by computer system. Besides, it enables the organisation to have technical control on software development and operation towards business continuity.

CSDP provides information security governance, risk management and cryptography as part of the security intelligent objectives and enhance security frameworks, legal regulation, cybercrime investigation and compliance by setting objectives for security operation, physical and environmental security. These enable the organisation to have both technical and management control on cyber security architecture, telecommunication, network security and the management control that focus on technology, people and leadership.

Besides that, the implementation of CSDP creates a platform for organisation Cyber Security Disaster Recovery (CSDR) which enables the organisation to resume business operation after cyber incident. It also enables the organisation to be resilience by creating cyber security events management team, network and digital forensic team, cyber security endpoint forensic team, cyber log management team, cyber security monitoring and response team. These teams enable organisation to focus on vulnerability intelligence analysis, cyber threats intelligence analysis, compliance and risk analysis, insider and outside threat analysis, advance persistence threat (APT) analysis, IT vendor analysis for effective incident recovery and mitigation.

Implementing CSDP means operating at the edge of security policies which will improve the organisation economic value due to Cyber Security Governance (CSG) provided. Governance involve the identification of both internal and external influences to the organisation (i.e. emerging technologies, social media, business environment, risk tolerance, regulatory requirements, third-party considerations, threat landscape) to ensure that these factors are continually addressed. Governance is all about IT leadership that focus on maintaining information security governance, to ensure organisational goals and objectives are supported by the information security program, to ensure security strategy are aligned with organisational goals and objectives to guide the establishment and improve the management of information security program which further create confidence to clients and stakeholders.

The implementation of CSDP will also improve the overall management of security practices because, it will enable the organisation to use the Cyber Security Risk Management (CSRM) to a better advantage by improving technical report on non-compliance and other changes in information risk. This is to facilitate the risk management decision-making process through appropriate and effective management of risk to an acceptable level and standards, monitor the internal and external factors using risk indicators, threat landscape, geopolitical and regulatory change. This may require reassessment of risk to ensure that changes to existing, or new risk scenarios are identified and managed appropriately. In order to manage risk to acceptable levels based on organisational risk appetite, appropriate risk treatment options can be implemented.

Cyber Security Management Program (CSMP) is another valuable component of the CSDP. It involves a program which focuses on security issues. It aligns security program with the operational objectives of other business functions (i.e. human resources, accounting, procurement and IT) to ensure that the security program adds value to and protects the business operations. It also promotes a program for Cyber Security Awareness and Training (CAT) to foster an effective security culture that includes people and technologies. This is done by compiling and present reports to key stakeholders on the activities, trends and overall effectiveness of the security management program and the underlying business processes in order to communicate security performance.

Cyber Security Incident Monitoring and Auditing (CSIMA) is another component within the CSDP. It complements other components as it relates to security monitoring and audit. Cyber Security Incident Monitoring and Auditing (CSIMA) is also one of the components within the CSDP. It works as a complement to other components as it relates to security monitoring and audit. Its benefits includes: 1) maintaining an organisational definition of severity hierarchy security incidents to allow accurate classification, 2) categorisation of response to incidents by creating opportunity for organisation to organise the level of risk i.e., low risk, medium risk and high risk, 3) training and equipping incident response teams to respond to security incidents in an effective and timely manner, 4) support to the organisation to conduct post-incident reviews to determine the root cause of incidents in other to develop corrective actions, reassess risk, evaluate response effectiveness, maintain communication plans and processes, 5) support to the organisation to manage communication with internal and external entities and maintain processes to investigate and document related to security incidents in order to determine the appropriate response.

Implementing CSDP, organisation will be able to test, review and revise incident response plan periodically to ensure an effective response to security incidents and to improve response capabilities, this enable the organisation to build security capability towards cybercrimes and cyber criminals. With the CSDP, organisation will be able to test, review and revise (as applicable) the incident response plan periodically to ensure an effective response to security incidents. Response capabilities are expected to improve and CSDP enables the organisation to build security capability towards cybercrimes and cyber criminals.

The CSDP is expected to provide basic set of security practices that are in conjunction with other relevant security practices. Therefore, from this study, it is posited that the proposed SCDP can be a tool for security controls and when adequately implemented can be effective in reducing cyber security risks on organisation asset.

VI. Conclusion

In achieving the objectives and established findings in the study, the following are applied: 1) SPSS data analysis that focus on descriptive analysis and standard multiple regression are applied to achieved the stated results, 2) eigenvalue analysis also known as factor analysis was applied to determine reliability on the seven identified principal components for the proposed CSDP, 3) survey questionnaire are set to determine the level of security practices and to identity the security practices from the selected organisations, 4) validation questionnaire are set based on the identified security practices from the selected organisations to be validated by 20 experts from security discipline.

The summary of findings in this study had revealed that implementing CSDP will cover a wide range of security management and create insight on how organisations should create an effective security policies to guide security practices. In comparison with prior studies, which shows that most organisations limit security practices according to their needs without considering other security factors or measures. The implementation of the proposed CSDP will create a wider security measure for organisation security program due to its seven principal components that are selected from a wide range of security program from reputable security organisations.

Limitations to this study are also identified in the area of data collections and the validation of the proposed CSDP. During data collections, not all the respondent respond to all questions, few questions are left out. These few unanswered questions are excluded from the data entry. Aside from these limitations, the 10 organisation for data collection and 20 experts for the validation of the proposed CSDP responded enough to suggest and make conclusion in this study that the proposed CSDP can be implemented as a cybersecurity policies and create a guidelines for organisations security practices.

From the data analysis outcome and validation of the proposed CSDP and the result from the eigenvalue analysis of the principal components for the proposed CSDP, it has shown that positive acceptance responds towards the proposed CSDP and that the proposed CSDP are significant enough for implementation, thus can be adopted by organisations as a guideline for organisation cyber security practices to mitigate cyber crimes and attacks.

In summary, from the identified cyber security practices from these 10 organisations, the harmonisation of the identified security practices to formulate cyber security defense polices (CSDP) and the validation of the proposed CSDP have been the achievements in this work.

The finding suggests that implementing CSDP cover a wide range of security management and create insight on how organisation should effectively manage and create security policies within security program. CSDP can also support organisation in testing, reviewing and revising incident response plan periodically to ensure an effective response to security incidents and to improve response capabilities towards cybercrimes, cyber criminals and cyber attacks simultaneously. This indicate a scientific value to cybersecurity program that is achieved in this paper.

In this case, this study recommends a new CSDP as a guideline for organisations cyber security practices and as it has been validated by experts from reputable organisations that have succeeded in cyber security policy implementation. In conclusion, it is highly recommended for organisations to implement a set of guidelines like the Cyber Security Defence Policies (CSDP) for managing and mitigating threats and put in place a governance that will govern how a system must be used.

VII. Future Work and Recommendation

Paying attention to cyber security is the most effective way to help the next generation understand the importance of virtual safety. Today, youngsters are at risk of numerous cyber threats ranging from hackers trying to encourage inadvertent disclosure of private information to individuals resorting to cyber bullying, harassment, and social embarrassment. A proactive approach towards cyber security will help the next generation imbibe lessons that will help them deal with such challenges in a confident and effective manner.

The ability to consistently classify information at all points in its life cycle and across the entire IT infrastructure is critical. If the information cannot be classified correctly, then it will not be able to be managed appropriately. Static classification of information by the information owner is not workable in today's global environment and so consistent automation is also required. In the future, Artificial Intelligent (AI) can be applied with some enhancement towards cyber security that will take account of machine learning and deep leaning, using python for large cyber security incident data-set to improve decision-making, knowledge sharing and to establish effective cyber security policies in organisations.

Acknowledgment

We would like to acknowledge and show our appreciation as this paper is supported by the Short Term Grant, Universiti Sains Malaysia (304/PKOMP/6315392).

References

[1] E. J. Murray and A. Durcikova, "Integrating IS security with knowledge management: Are we doing enough to thwart the persistent threat?" 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, 2014, pp. 3452-3459.

[2] N. Perlroth, M. Scott, and S.Frenkel, "Cyberattack hits Ukraine then spreads internationally," The New York Times, June 27, 2017, Accessed: October 5, 2019. [Online]. Available: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

[3] C. Skouloudi and M. Fernandez, "Towards secure convergence of cloud and IoT," The European Union Agency for Cybersecurity (ENISA), September 17, 2018, Accessed: October 5, 2019. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/towards-secure-convergence-of-cloud-and-iot

[4] M. P. Barrett, "Framework for Improving Critical Infrastructure Cybersecurity Version 1. 1," April 16, 2018, Accessed: October 24, 2019. [Online]. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

[5] S. Mittal, "Knowledge for cyber-threat intelligence," Ph.D. dissertation, Univ. of Maryland, MD, USA, 2019.

[6] E. O. Yeboah-Boateng and E. Akwa-Bonsu, "Cyber-security intelligence gathering: Issues with knowledge management," in Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, IGI Global, 2018, pp. 1454-1479.

[7] T. Poppensieker and R. Riemenschnitter "A new posture for cybersecurity in a networked world," in Perspectives on transforming cybersecurity, Digital McKinsey and Global Risk Practice, 2019, pp. 18-26.

[8] K. Min, C. S. Chai, and M. Han, "An international comparative study on cyber security strategy," International Journal of Security and its Applications, vol. 9(2), 2015, pp. 13-20.

[9] D. Manky, "Threats in the information age," in Cyber Security Threats, Challenges and Opportunities, Australian Computer Society, 2018, pp. 14-15.

[10] P. S. Seemma, S. Nandhini, and M. Sowmiya, "Overview of cyber security," International Journal of Advanced Research in Computer and Communication Engineering, vol. 7(11), 2018, pp.125-128.

[11] B. Mat, S. D. M. Pero, R. Wahid, and B. Sule, "Cybersecurity and digital economy in Malaysia: Trusted law for customer and enterprise protection," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8(8S3), 2019, pp. 214-220.

[12] CSIS, "Net losses: Estimating the global cost of cybercrime. Economic impact of cybercrime II", CSIS (Centre for Strategic and International Studies), June 5, 2014, Accessed: [Online]. Available: https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime

[13] S. McKune, "An Analysis of the International Code of Conduct for Information Security", Citizen Lab, September 28, 2015, Accessed: June 26, 2018 [Online]. Available: https://citizenlab.ca/2015/09 /international-code-of-conduct/

[14] E. Minei and J. Matusitz, "Cyberspace as a new arena for terroristic propaganda: an update examination," International Journal of Ethics of Science and Technology Assessment, vol. 9(1), 2012, pp. 163–176.

[15] L.M. Rhode, "Human traficking as cybercrime," AGORA International Journal of Administrative Science, vol. 1(1), 2017, pp.23-29.

[16] M. N. Katsantonis, I. Kotini, P. Fouliras and I. Mavridis, "Conceptual framework for developing cyber security serious games," In Global Engineering Education Conference (EDUCON) 2019 IEEE, pp. 872-881, Dubai, United Arab Emirate, 2019.

[17] M. Mahmud, M. S. Kaiser, M. M. Rahman, M. A. Rahman, A. Shabut, S. Al-Mamun and A. Hussain, "A brain-inspired trust management model to assure security in a cloud based IoT framework for neuroscience applications" Journal of Cognitive Computation. vol.10, 2018, pp. 864-873.

[18] T. Poppensieker and R. Riemenschnitter, "A new posture for cybersecurity in a networked world," in Perspectives on transforming cybersecurity, D.Chinn, J. M. Kaplan, and T. Poppensieker, Digital McKinsey and Global Risk Practice, 2019, pp. 18-26.