Development of a Cyber Security Awareness Strategy Using Focus Group Discussion

Zahri Yunos[1], Ramona Susanty Ab Hamid[2], Mustaffa Ahmad[3]
CyberSecurity Malaysia
Selangor, Malaysia
zahri@cybersecurity.my[1], ramona@cybersecurity.my[2], mus@cybersecurity.my[3]

***Abstract*—Focus group discussion is often used as an exploratory technique and serves as a source of data collection. It typically consists of a group of 5 to 10 participants led by a moderator. This work contributes to developing a cyber security master plan in Malaysia through focus group discussion. For this study, thirty-two (32) participants took part in focus group discussions. The background of the participants varied from management, policy-making, law enforcement and prosecution to the research and technical fields. The participants had a range of working experience. The target groups identified are kids, youths, adults and parents, and organizations (both public and private sectors). The overall results suggest that in order to achieve a successful cyber security awareness implementation strategy, three implementation layers are recommended: strategic, program execution and content development layers. The findings provide a holistic approach to developing a single common platform for cyber security awareness programs in Malaysia that encompasses various stakeholders.**

Keywords—Cyber Security Awareness; Cyber Security; Focus Group Discussion

I. Introduction

A more holistic way of describing cyber security awareness would be useful to attain effective cyber security awareness programs. A common understanding of this term is important to better comprehend what constitutes cyber security awareness. Enhancing cyber security awareness is a major goal for many organisations, whereby greater awareness of the state of environments enables improved decision-making. As there are many definitions of cyber security awareness, it is suggested that further analysis of the phenomenon be conducted.

Awareness, as defined by the EC-Council under the Certified Chief Information Security Officer, "stimulates and encourages those being trained to take care about information security and to continually remind them of important security practices" [1]. Awareness is a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure. This is explicitly required in all aspects of life. Awareness is extremely important in the ICT security sphere, because a person's actions can affect an entire organization. Lack of awareness from the person responsible can cause serious damage and loss to an organization.

Cyber security awareness is all about conveying information and best practices to specific target groups. Cyber security awareness programs address how and what sorts of materials and tools can be used to convey messages and that make such programs successful and impactful or failures. It is the multidimensional structure of an awareness program itself that makes people interpret it differently at various levels. Therefore, understanding what constitutes effective cyber security awareness is imperative.

II. Method

A. *Background of this study*

The focus group discussion was conducted in two (2) series of a 2-day workshop. The discussion was designed as a platform to address cyber security awareness programs from a holistic approach. The workshop provided basic insight into cyber security programs that are currently conducted by various agencies, threats, issues and challenges revolving around conducting programs, as well as complexities in coming up with, and developing program materials. Stakeholders from various agencies who are responsible for deploying cyber security awareness programs were invited to share their thoughts and perspectives on this topic on the first day of the workshop. In addition, the moderator presented a detailed explanation of the national cyber security awareness program master plan on the 1st day of the workshop. The sessions were designed in such a way so as to trigger the participants' thoughts and to channel all relevant matters to the focus group discussion.

B. *Participants*

Focus group discussion often serves as an exploratory technique and is a source of data collection [2] [3]. It is an adequate method of obtaining information about the ideas, feelings, attitudes and preferences of a target group [4]. Focus group discussion normally consists of a group of 5 to 10 participants led by a moderator [5]. Focus group research, as a qualitative method, enables participants to elaborate and engage in dialogue with one another [6]. Focus group discussions can help gain more insight into what is already known and this information can be added to the current discussion about cyber security awareness. In addition, focus group discussions generate evidence that is commonly applied to evaluating diverse programs and policies.

For this study, 32 participants took part in the focus group discussions. They were divided into smaller groups of 6 to 7 participants each. This approach is similar to the focus group discussions conducted by Bray, Johns and Kilburn [7]. The

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

participants included managers, policy makers, law enforcement and prosecution experts, researchers and technical experts, all having a range of working experience between 5 and 20 years. All participants were from government agencies, private sectors, academia and NGOs. The distribution of participants is tabulated in Table I.

TABLE I. DISTRIBUTION OF PARTICIPANTS

Distribution by Sector	# of Organisations	# of Participants
1. Public Sector	8	10
2. Private Sector	5	6
3. Regulators	5	8
4. Higher Learning Institution	1	1
5. NGOs	5	7
Total	24	32

C. *Procedure*

The participants were divided into 5 groups, who differed in terms of age, organization and working experience. The rationale behind having smaller groups is to give everyone the opportunity to express their views and opinions. The groups were based on target groups: kids, youths, adults/parents, Critical National Information Infrastructure (CNII) organizations and non-CNII organizations.

A briefing session was conducted to ensure that each focus group followed the same structure and had the same understanding of the key objectives and discussion guidelines. Each group was given a flip chart on which to write their discussion points during the group brainstorming session. Before the group discussion, the proposed national cyber security awareness program master plan and what the group should explore were explained: mission, vision, objectives, concept, target groups, enablers, funding, domain/supporting pillars, methods, impact, roles and responsibilities, capacity building and governance structure.

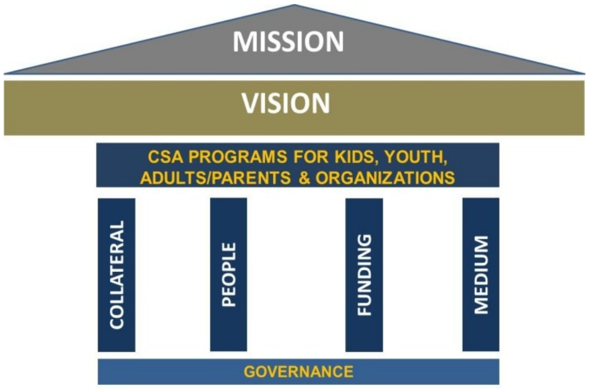

MISSION
VISION
CSA PROGRAMS FOR KIDS, YOUTH, ADULTS/PARENTS & ORGANIZATIONS
COLLATERAL
PEOPLE
FUNDING
MEDIUM
GOVERNANCE

Fig. 1. Proposed National Cyber Security Awareness Master Plan framework

Focus group discussion was identified as an appropriate and accessible technique given the exploratory research nature [7]. The objectives of the focus group discussion were as follows: first, to discuss factors that entail cyber security awareness program components and secondly, to evaluate the proposed conceptual master plan that describes the cyber security awareness program components. In a nutshell, the focus group discussion was conducted to achieve consensus on people's perceptions of the proposed national master plan for a national cyber security awareness program. The framework of the proposed national cyber security awareness master plan is presented in Fig. 1.

The primary output of this work was gauging the participants' views of the proposed national cyber security awareness master plan. A moderator facilitated the focus group discussions by providing guidance to the group and allowing respondents to talk freely and spontaneously when expressing ideas, views and experiences on a given topic. Although the moderator initiated the discussion topic and thus exercised certain control over what was to be discussed, he did not offer any perspectives during the talk-in-process session. As recommended by Bray, Johns and Kilburn [7], a relaxed and conversational method was applied during the focus group discussion in order to produce a free-flowing conversation with minimum moderator intervention.

Kamarulzaman [8] explained that in a focus group, people interact with each other with the help of a moderator to obtain more information and share their own experiences. It is noted that the usefulness of focus group data is affected to the extent that the participants are openly communicating their ideas, views, or opinions during the focus group discussions. This is ascertained by Ho [3], who explained that people gather together to voice their opinions and perceptions about a study topic in a comfortable environment. During the discussion, participants are encouraged to talk to one another; they are asked questions and exchange comments on the group's presentation. The focus group study allows a flexible and in-depth exploration of participants' attitudes and experiences and also reveals differences in perspectives between groups of individuals [9].

TABLE II. SAMPLE QUESTIONS FOR THE FOCUS GROUP DISCUSSIONS

Q1. Does your agency have or is it implementing a Cyber Security Awareness Program? (Yes or No answer)

Q2. Please list down the details of the Cyber Security Awareness (CSA) programs/initiatives that your agency has carried out in the past 3 years up to the present:

Q3. What are the main contents of each program delivered?

Q4. What is the feedback/response gathered about the programs conducted? How was feedback gathered?

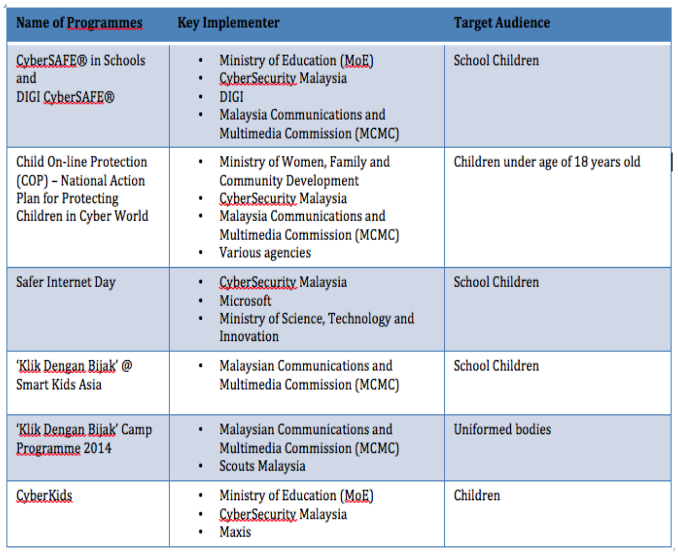
In terms of context setting, the participants were asked several questions (Table II) with focus on cyber security awareness programs. The questions were not run in any sequential order to provide guidelines and overviews on the topic under discussion.

D. *Data Collection*

Prior to the focus group discussions, separate discussions were conducted to explore the concept of a cyber security awareness program master plan. Meaning to say, the focus

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

group discussions were conducted in addition to in-depth discussions to explore the concept of a cyber security awareness program. The group discussions were recorded and the discussion points that were noted on the template were collected at the end of the sessions.



Name of Programmes	Key Implementer	Target Audience
CyberSAFE® in Schools and DIGI CyberSAFE®	• Ministry of Education (MoE) • CyberSecurity Malaysia • DIGI • Malaysia Communications and Multimedia Commission (MCMC)	School Children
Child On-line Protection (COP) – National Action Plan for Protecting Children in Cyber World	• Ministry of Women, Family and Community Development • CyberSecurity Malaysia • Malaysia Communications and Multimedia Commission (MCMC) • Various agencies	Children under age of 18 years old
Safer Internet Day	• CyberSecurity Malaysia • Microsoft • Ministry of Science, Technology and Innovation	School Children
'Klik Dengan Bijak' @ Smart Kids Asia	• Malaysian Communications and Multimedia Commission (MCMC)	School Children
'Klik Dengan Bijak' Camp Programme 2014	• Malaysian Communications and Multimedia Commission (MCMC) • Scouts Malaysia	Uniformed bodies
CyberKids	• Ministry of Education (MoE) • CyberSecurity Malaysia • Maxis	Children

Fig. 2. Programs of various agencies

Apart from the discussions, input from other agencies was obtained through survey. More than 30 government agencies, private institutions and NGOs conduct various programs, either on a large or small scale within their entity. The survey results are shown in Fig. 2. It is worth noting that programs conducted by the agencies are from their own initiatives. Some of the programs are collaborations with other agencies but most are work in silo.

III. Results

A. Views on existing programs and how to elevate them

Similarities and differences help shed light on the matters under discussion as well as provide a pathway for better analysis of the findings [10]. In this work, similarities among the 5 groups are analysed. All groups agreed that a lack of coordination leads to working in silo. When the program is run on its own, program implementation is only focused on one target group repeatedly. There is no coordination and communication among the agencies; hence, the program becomes redundant. Since the group was divided into different target groups, each individual finding is assessed accordingly.

All five (5) groups agreed that a cyber security awareness program master plan needs to be tightly aligned and concerted in both effort and coverage. Group 1, which concentrated on kids, indicated that a vision for the future should embed cyber security awareness into school curriculums or subjects. Besides school curriculum, there should be a one-stop centre or portal, where end users can retrieve content meant for kids. It was also brought to attention that children need to know their rights for protection online and must be aware of reporting platforms.

Group 2, who looked at youths, stressed on some enablers, whereby buy-in and prioritization need to be obtained from key stakeholders. The group felt that in order to drive cyber security program implementation, besides being able to provide a successful and impactful program, getting buy-in and prioritization from key stakeholders is important. The group also suggested developing equipment, tools and facilities for youth, minorities and marginalized groups. Group 3, who focused on adults, pointed out that adults should emphasize on responsibility, accountability, safeguarding, education, ethics and morals.

Groups 4 and 5 concentrated on the public and non-government sectors, respectively. Group 4 proposed programs that should be done periodically, as these will constantly engage audiences in order to increase awareness levels. This can be done via planned and structured campaigns. A structured campaign that an organization can participate in is the Human Impact Management System for Information Security (HIMIS) program. HIMIS is a study that can manage individual levels of understanding of cyber security. Both groups proposed capacity building and professional training, which highlight continuous improvement and facilitate up-to-date information.

B. Views on the Findings: SWOT vs Strategies

The major findings regard lack of coordination; lack of funding; content availability; and impact assessment. The analysis is based on SWOT, and in each quadrant, the findings are categorized into 4 main strategies, namely Emphasize, Reinforce, Develop and Must-have. The interrelations between SWOT and the Strategies are shown in Fig. 3.

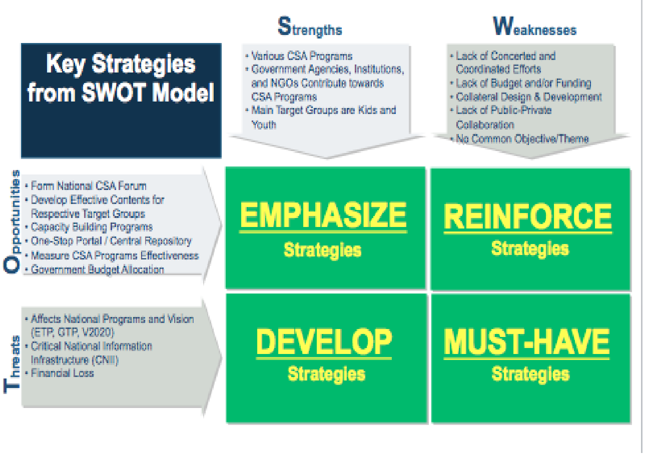

Strengths
Weaknesses
Key Strategies from SWOT Model
• Various CSA Programs
• Government Agencies, Institutions, and NGOs Contribute towards CSA Programs
• Main Target Groups are Kids and Youth
• Lack of Concerted and Coordinated Efforts
• Lack of Budget and/or Funding
• Collateral Design & Development
• Lack of Public-Private Collaboration
• No Common Objective/Theme
Opportunities
• Form National CSA Forum
• Develop Effective Contents for Respective Target Groups
• Capacity Building Programs
• One-Stop Portal / Central Repository
• Measure CSA Programs Effectiveness
• Government Budget Allocation
EMPHASIZE
Strategies
REINFORCE
Strategies
Threats
• Affects National Programs and Vision (ETP, GTP, V2020)
• Critical National Information Infrastructure (CNII)
• Financial Loss
DEVELOP
Strategies
MUST-HAVE
Strategies

Fig. 3. Interrelations between SWOT and Strategies

The findings from all focus groups were analysed and described in Figures 4, 5, 6 and 7. Quadrant one (1) represents Emphasize Strategies, Strengths vs. Opportunities (Fig. 4). Under strengths, it is known there are various cyber security awareness programs led by different government agencies, institutions and NGOs.

However, the targets are rather kids and youths. Thus, there are opportunities to form a national cyber security awareness forum to monitor the implementation of each awareness program. Apart from creating a forum, it would be possible to develop more effective and meaningful content geared more towards other groups.

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

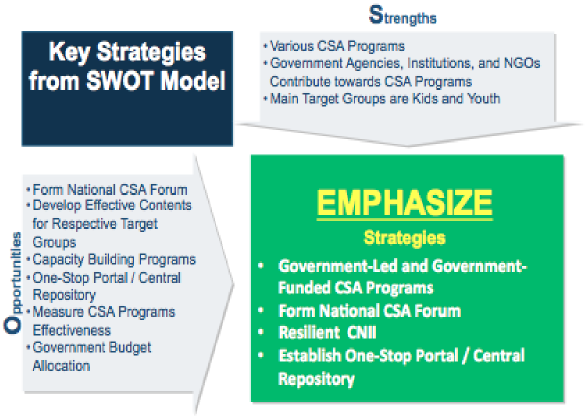

Strengths
Key Strategies from SWOT Model
•Various CSA Programs
•Government Agencies, Institutions, and NGOs Contribute towards CSA Programs
•Main Target Groups are Kids and Youth
Opportunities
•Form National CSA Forum
•Develop Effective Contents for Respective Target Groups
•Capacity Building Programs
•One-Stop Portal / Central Repository
•Measure CSA Programs Effectiveness
•Government Budget Allocation
EMPHASIZE
Strategies
• Government-Led and Government-Funded CSA Programs
• Form National CSA Forum
• Resilient CNII
• Establish One-Stop Portal / Central Repository

Fig. 4. Interrelation between Strengths vs. Opportunities - Emphasize Strategies

Next is Develop Strategies (Fig. 5). According to the analysis findings, there are some threat elements that require attention. Many effective contents need to be developed to address the respective target groups.

Upon local content development, local talents and experts are also in high demand, thus capacity-building programs must be developed to train local expertise.

This can be done via collaboration programs with Institutes of Higher Learning Centres, scholarship offers, and the development of suitable curriculums for schools. Localizing international content to suit local scenarios can also be developed.

The third (3^{rd}) quadrant addresses Reinforce Strategies with Weakness vs. Opportunity (Fig. 6). It is understood that over the past years there has been a lack of concerted and coordinated effort. Secondly, in terms of budget and funding, a lack of these leads to 'touch and go' programs with no continuity.

Lack of budget and funding also contribute to the lack of collateral development. Besides lacking concerted and coordinated effort, the lack of public-private collaboration with no common objectives/themes is another weakness. With all the listed weaknesses, it can be concluded that elements that need reinforcement include improving existing programs, adopting effective programs and aligning programs with the national programs and vision.

The last quadrant of Must-have Strategies is the most important and necessitates the most attention, as the items highlighted are weaknesses vs. threats (Fig. 7). Thus, must-have strategies can be proper cyber security awareness program planning, coordination and execution. Each program must have effective program evaluation in order to assess the impact and return of investment. With such results, agencies would be able to justify requests for additional funds and budgets.

In conclusion, the need for a master plan arises in order to address cyber security awareness program implementation at the national level.

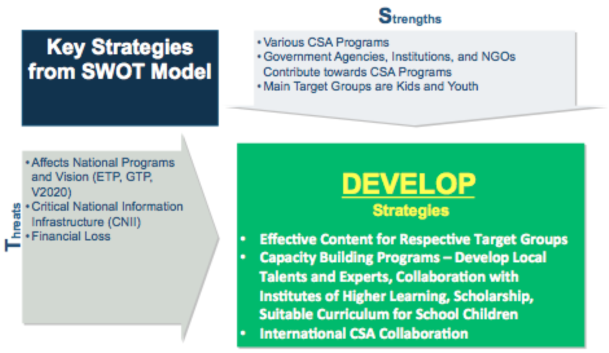

Strengths
Key Strategies from SWOT Model
•Various CSA Programs
•Government Agencies, Institutions, and NGOs Contribute towards CSA Programs
•Main Target Groups are Kids and Youth
Threats
•Affects National Programs and Vision (ETP, GTP, V2020)
•Critical National Information Infrastructure (CNII)
•Financial Loss
DEVELOP
Strategies
• Effective Content for Respective Target Groups
• Capacity Building Programs – Develop Local Talents and Experts, Collaboration with Institutes of Higher Learning, Scholarship, Suitable Curriculum for School Children
• International CSA Collaboration

Fig. 5. Interrelation between Strengths vs. Threats - Develop Strategies

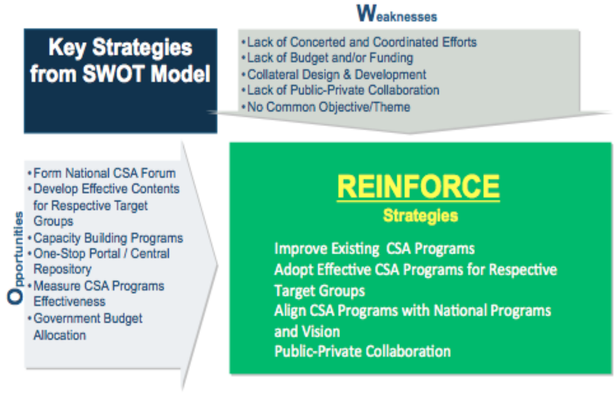

Weaknesses
Key Strategies from SWOT Model
•Lack of Concerted and Coordinated Efforts
•Lack of Budget and/or Funding
•Collateral Design & Development
•Lack of Public-Private Collaboration
•No Common Objective/Theme
Opportunities
•Form National CSA Forum
•Develop Effective Contents for Respective Target Groups
•Capacity Building Programs
•One-Stop Portal / Central Repository
•Measure CSA Programs Effectiveness
•Government Budget Allocation
REINFORCE
Strategies
Improve Existing CSA Programs
Adopt Effective CSA Programs for Respective Target Groups
Align CSA Programs with National Programs and Vision
Public-Private Collaboration

Fig. 6. Interrelation between Weaknesses vs. Opportunities - Reinforce Strategies

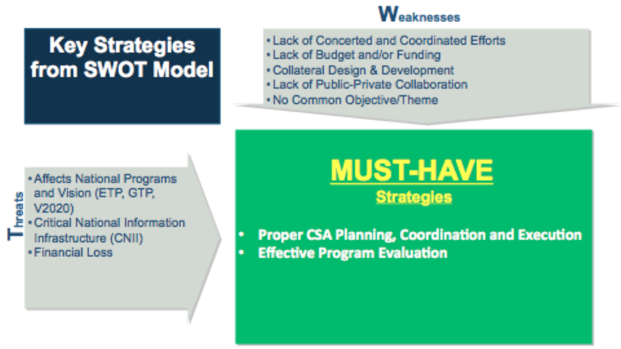

Weaknesses
Key Strategies from SWOT Model
•Lack of Concerted and Coordinated Efforts
•Lack of Budget and/or Funding
•Collateral Design & Development
•Lack of Public-Private Collaboration
•No Common Objective/Theme
Threats
•Affects National Programs and Vision (ETP, GTP, V2020)
•Critical National Information Infrastructure (CNII)
•Financial Loss
MUST-HAVE
Strategies
• Proper CSA Planning, Coordination and Execution
• Effective Program Evaluation

Fig. 7. Interrelation between Weaknesses vs. Threats - Must-Have Strategies

C. *Views on the Proposed National Cyber Security Awareness Program*

An implementation structure was proposed after receiving comments and feedback from the participants. The structure was developed into 3 layers, namely Strategic, Program Execution and Content Development (Fig. 8). The first is the strategic layer, which reflects the vision of how Cyber Security Awareness (CSA) initiatives are planned and of strategies before being rolled out. The National CSA Forum is the governing body for planning, strategizing and overseeing the overall direction of CSA initiatives. This national forum is a coalition between government agencies, private sectors,

978-1-4673-8460-5/16/$31.00 ©2016 IEEE

community organizations as well as industry experts in the respective fields to deliver more effective CSA program content to each target group. When it comes down to target group coordinators, agencies that have the ability to lead and take ownership will be coordinators and planners.

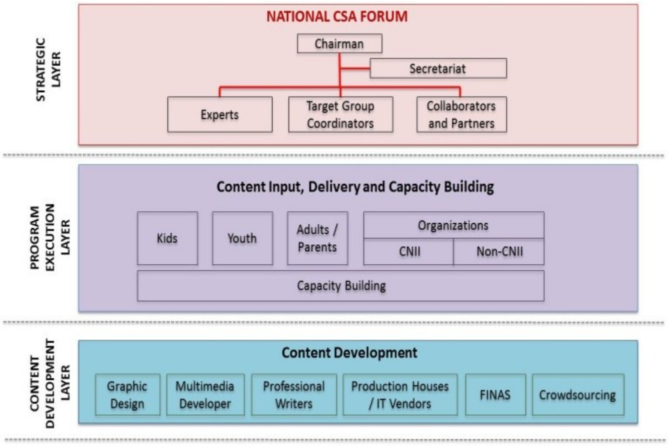


Fig. 8. Cyber Security Awareness (CSA) Strategy

The second layer is the program execution layer. The main objective of this layer is to set up a workable process for input gathering and content dissemination to the correct target groups identified. One of the recognized methods is to leverage on the agency/organization channel to disseminate awareness messages regarding cyber security. On a side note, capacity building is included in this layer to develop a pool of trainers for the awareness program and to ensure cyber security awareness program sustainability. Apart from this, all content developed will be parked in the national repository centre. The content can be used freely by agencies registered with the forum. The third, content development layer is responsible for the development of effective cyber security awareness collateral/material for the identified target groups. The same awareness topic delivered to different target audiences will most likely require different content and media. Some of the agencies that attended the workshop expressed they do not have the capabilities to develop and produce content. They further explained that they lack the expertise to develop content suitable for the right audience. Thus, it is recommended to establish a dedicated group who can develop the right content that matches the target audience. The content development layer is like a production house. Content can be videos, posters, modules or even curriculum modules for schools. The finished product will be stored in the central repository.

IV. Research Limitations

This study has some limitations, which may lead to the unreliability of the data collected [11]. A constraint of this study is that the majority of participants were representatives from agencies, NGOs and government sectors. However, only few CNII agency representatives attended. Malaysia has 10 CNII sectors: water, banking & finance, defence & security, transportation, information & communication, government, emergency services, food & agriculture, energy, and health. Therefore, the focus group discussion participants did not represent all CNII sectors as a whole.

V. Conclusion

Cyber security awareness programs are significant and require concerted effort to avoid program redundancy. It is important to reach out to all target groups without favouritism or repetition. Besides, local content ought to be enhanced to suit the local scenario. Although there are differences in opinions on some of the components, overall the views were not extremely critical and can be further justified. It is known this is the first time such work has been conducted in Malaysia. The workshop formulated a comprehensive cyber security awareness program master plan for Malaysia.

The master plan covers wide areas of elements and groups of communities, including youth, minorities and marginalized groups. Hence, there must be mutual understanding between stakeholders. Having an ongoing security awareness program in place can greatly reduce the risks of security breaches. It is recommended for awareness to be inculcated in an organization to ensure good security practices through mandatory policies or executive orders. In addition, management should play a very distinctive role in the establishment of well-defined awareness policies. Net citizens need protection against perpetrators with ill intentions and who use opportunities on the gullible and naïve. With a comprehensive master plan, a solid cyber security awareness program could be possible, which would touch as low as the grass root and as high as the top of the pyramid.

References

[1] EC-Council Official Courseware. Certified Chief Information Security Officer, 2015.

[2] D. W. Stewart and P. N. Shamdasani, Focus Groups: Theory and Practice. Sage Publications, 2014.

[3] D. Ho, “The Focus Group Interview: Rising to the Challenge in Qualitative Research,” Aust. Rev. Appl. Linguist., vol. 29, no. 1, pp. 1–19, 2006.

[4] N. C. L. Jacobs, L. Goossens, F. Dehue, T. Völlink, and L. Lechner, “Dutch Cyberbullying Victims’ Experiences, Perceptions, Attitudes and Motivations Related to (Coping with) Cyberbullying: Focus Group Interviews,” Societies, vol. 5, no. 1, pp. 43–64, 2015.

[5] B. Beckert, S. Grebing, and F. Böhl, “How to Put Usability Into Focus: Using Focus Groups to Evaluate the Usability of Interactive Theorem Provers,” in Eleventh Workshop on User Interfaces for Theorem Provers, 2014, pp. 4–13.

[6] C. Hu, H. Pazaki, and E. Velander, “Evaluating Global Education at a Regional University: A Focus Group Research on Faculty Perspectives,” Theory in Action, vol. 7, no. 1, p. 65, 2014.

[7] J. Bray, N. Johns, and D. Kilburn, “An Exploratory Study into the Factors Impeding Ethical Consumption,” J. Bus. Ethics, vol. 98, no. 4, pp. 597–608, 2011.

[8] Y. Kamarulzaman, “A Focus Group Study of Consumer Motivations for e- Shopping : UK versus Malaysia,” African J. Bus. Manag., vol. 5, no. 16, pp. 6778–6784, 2011.

[9] F. Saleem, M. Hassali, A. Shafie, S. Bashir, and M. Atif, “Perceptions of Disease State Management Among Pakistani Hypertensive Patients : Findings from a Focus Group Discussion,” Trop. J. Pharm. Res., vol. 10, no. 6, pp. 833–840, 2011.

[10] B. Perelli-Harris, M. Mynarska, A. Berrington, and C. Berghammer, “Towards a New Understanding of Cohabitation : Insights From Focus Group Research Across Europe and Australia,” Demogr. Res., vol. 31, no. 34, pp. 1044–1078, 2014.

[11] D. R. Cooper and P. S. Schindler, Business Research Method. NY: McGraw-Hill Companies, Inc, 2008.