UNIVERSITI TEKNOLOGI MARA
Cawangan Kedah
Kampus Sungai Petani

2021 iCMS
INTERNATIONAL CONFERENCE ON COMPUTING, MATHEMATICS AND STATISTICS

e-PROCEEDINGS

of The 5th International Conference on Computing, Mathematics and Statistics (iCMS2021)

4-5 August 2021

Driving Research Towards Excellence

2021 iCMS

INTERNATIONAL CONFERENCE ON COMPUTING,
MATHEMATICS AND STATISTICS

e-Proceedings of the 5th International Conference on Computing, Mathematics and Statistics (iCMS 2021)

Driving Research Towards Excellence

e-ISBN: 978-967-2948-12-4
DOI

Library of Congress Control Number:

The views and opinions and technical recommendations expressed by the contributors are entirely their own and do not necessarily reflect the views of the editors, the Faculty or the University.

Publication by
Department of Mathematical Sciences
Faculty of Computer & Mathematical Sciences
UiTM Kedah

TABLE OF CONTENT

PART 1: MATHEMATICS

PART 2: STATISTICS

PART 3: COMPUTER SCIENCE & INFORMATION TECHNOLOGY

PART 4: OTHERS

Information Security Culture: A Qualitative Approach on Management Support

Qamarul Nazrin Harun[1], Mohamad Noorman Masrek[2], Muhamad Ismail Pahmi[2] and Mohamad Mustaqim Junoh[3]*

[1] Faculty of Information Management, Universiti Teknologi MARA, 85000 Segamat, Johor, Malaysia

[2] Faculty of Information Management, Universiti Teknologi MARA, 40150 Shah Alam, Selangor Malaysia

[3] Faculty of Computer & Mathematical Sciences, Universiti Teknologi MARA, 85000 Segamat, Johor, Malaysia

*Corresponding author : mustaqimjunoh@gmail.com

Abstract

In the Industrial Revolution 4.0 (IR 4.0), information security has been highlighted as one of the critical components that needs to be addressed by industry practitioners. To this effect, the deployment of information security controls, both technical and nontechnical is very essential so as to safeguard and protect organizational information from any form of threats or danger. Information Security Culture (ISC) is a term used to describe a situation where not only members aware and skillful in terms of information security, but the process and procedure as well as the technologies are also in place to protect and safeguard organizational information. This paper reports the findings of a study aimed at assessing the ISC of the Malaysian public organizations. The study used a survey research methodology with a questionnaire as the data collection technique. The results of the study suggest that ISC which are measured in terms of management support, policy and procedures, compliance, awareness, budget and technology are not in place in these participating organizations. The findings send a strong message that much effort is needed to strengthen the ISC in these participating organizations.

Keywords: information security culture, malaysian public organization, management support, qualitative, unstructured interview.

1 Introduction

The COVID-19 pandemic has forced the world to accelerate the digitalization process. Entering to this new era of fourth industrial revolution (IR4.0) and digilatization, the Malaysian organization is required to be secure, vigilant, and resilient to the evolution of information security threats. This is due to the fact that a total of 10,790 information security incidents were reported in 2020, compared to 9,915 information security incidents in 2015 (MyCERT, 2020). Cybercriminals have targeted the government sector to carry out various attacks with various purposes. Security threats that occur will cause the organization's image to be contaminated thereby affecting the organization's performance. The stakeholders will have the perception that the organization has weak management so as not to be able to ensure that the organization is safe from any threat of information either from outside or within the organization itself. As a result, stakeholders such as investors will not take the risk of investing in the government, thereby negatively affecting the country's economic growth. Due to the information security incidents keep occurring regularly, especially in public organizations which are the key to the development of a country, management has to take effective and efficient measures to protect critical information within the organization.For decades, scholars have agreed that managerial attention plays an important role in solving information security issues that occur within the organization (Allen, 1968; Parker and Gardetto, 1981; Tassel, 1972). However, managers usually do not see information security is important and should be noted. Therefore, the security management of information assets in the organization is not specifically addressed. (Straub, 1990).

Since the internet was introduced in the organization in early 2000, most organizations have started migrating the way management uses information technology as a basis for achieving the organization's objectives. However, the rapidly expanding technological developments have also increased the threats of information security such as e-mail viruses, worms, and software vulnerabilities. Unfortunately, managerial attention to strengthen the security of information assets in the organization remains insufficient due to the constant threat of information security. Awareness of the role of organizational management in protecting information assets should be enhanced due to the management or leadership of an organization plays a very important role to cultivate the work culture that will enhance the information security culture (ISC) within the organization. A total of 874 certified information security professionals have stated that top management support is seen first in the list of 25 security issues (Knapp et al., 2009). This suggests that security incidents occurring within the organization are attributed to top management who do not pay attention to the management of information security especially the establishment of ISC within the organization. Looking at the need for guidance on creating ISC, especially in the aspect of management support in public organizations, many researchers have focused on building an ISC model within the organization. However, the ISC model in the context of Malaysian public organization is still limited and immature. Therefore, this study aims to identify dimensions of ISC of Malaysian public organization and to assess the state of practices of ISC of Malaysian public organization. Then, this paper will focus more on managerial aspects that play an important role in establishing ISCs in Malaysia's public organization.

Literature studies have been conducted to answer the first research objective to identify dimensions of ISC that are often used to foster ISC within the organization. Subsequently, qualitative study was directed to identify the suitability of ISC dimensions obtained from literature studies in Malaysian public organization settings as well as to examine the state of practices of ISCs of Malaysian public organization. Overall, the findings from the qualitative studies that have been conducted have confirmed the literature findings which six dimensions of ISC were suitable to be implemented in the context of Malaysia public organization, namely Management Support, Policy and Procedure, Compliance, Awareness, Budget and Technology, but only the domain Management Support to be touched in this paper. Other dimensions will be spared in the future. This paper also is organized into seven sections. The first section describes the overview of ISC. The second section discusses the literature review and conceptual framework. The third section highlights the methodology used in the study. Next section deliberates the results of the study. Following that, discussion from the analysis conducted were discussed. This paper is wrap up with conclusion and acknowledgement.

2 Literature Review and Conceptual Framework

Various angles within the ISC domain have been explored by many researchers to understand deeper in order to contribute to the body of knowledge in the aspect of social science to the world. Furthermore, it can be used as a guide by organizations to equip their organizations with information security features practice as a second nature. Among them are Mahfuth et al. (Mahfuth et al., 2017). They have understood the ISC as "employees' perceptions that interact with information assets in an organization are driven or influenced by security behaviour that are managed through a process of integration of beliefs, perceptions, attitudes, values, assumptions and knowledge of information security". Through this understanding, it can be seen that human factor plays an important role in determining any action in every matter whether to be a 'human firewall' that retains information from an unauthorized people or is the cause of an information security threat. This is in line with European Union Agency for Network and Information Security (ENISA) (ENISA, 2018) which stated that most information security incidents were caused by human factor. They also added that the damage occurring within the organization was often due to the underlying policy imperatives that have resulted in misuse in the handling of information security technology. In addition, the resilient of information security can exist if there is an ISC that affecting employees within the organization (Beaver, 2015).

For that, management should play their role as a leader in the organization to shape the attitude of employees through the establishment of ISC. Integration built between management and employees can create a strong culture in terms of information security. This is because of management involvement in every activity within the organization will affect the behavior of employees (Romeo, 2021).

In the context of Malaysia public organization, information security incidents are seen to be at an alarming level. Earlier in 2018, the country was once again surprised by the leakage of online information involving 200,000 organ donors' personal information. According to (A and M, 2018), leakage of organ donor information is believed to be stolen from the central database and has various information such as patient records, addresses, and identity card numbers and so on. Donor data donor organ is at risk for cyber criminals to use as false information for cybercrime. Additionally, the Ministry of Education's School Examination Analysis System (SAPS) portal aimed at analyzing the results of school student examinations has been reported to have a security escalation that potentially reveals more than 10.3 million personal information of students and parents (Ar, 2018). Data involving MyKad's number of schoolchildren, parental identification number, parental address and parental status, which in turn gives access to the entire family unit. The leakage of this information is also due to the weakness of the system that does not address security features where hackers can steal information easily. Looking at these information security incidents, it is a priority for Malaysia public organizations to focus more on information security. Especially in social aspects. And it is the responsibility of management to ensure that information security is prioritize in every activities and actions so that the risk of information security incidents can be minimized. Through implementation of ISC in Malaysia public organization is seen to be able to create a principle in every employee to make information security as a key indicator before making any action.

In order to further enhance the ISC in the context of Malaysian public organization, adopting the conceptual framework developed by (Masrek et al., 2018), Figure 1 showcases the conceptual framework of ISC of Malaysia public organization. It consists of six dimensions and each one of them has two elements. Namely, Management Support (Information Security Commitment and Information Security Importance), Policy and Procedure (Information Security Policy Effectiveness and Information Security Directives), Compliance (Information Security Monitoring Perception and Information Security Consequences), Awareness (Information Security Responsibility and Information Security Training), Budget (Information Security Budget Practice and Information Security Investment) and Technology (Information Security Technology Compatibility and Information Security Technology Capability). Malaysia public organization will be able to create a solid ISC if all these dimensions and elements are coexist and being implemented together. In addition, this conceptual framework was developed by grouped all the dimensions in two separate sets of perceived importance to identify the dimensions of ISC that are suitable for practice in the context of Malaysian public organization and perceived implementation to see how far each dimensions have been practiced in Malaysia public organization.

3 Methodology

Table 1 presents the demographic profiles of the participants who were involved in the study. A total of seven (7) participants were interviewed. These participants were attached to Prime Minister's Office, Ministry of Education, Ministry of Science, Technology and Innovation, Ministry of Home Affairs and Ministry of Communications and Multimedia. Of 7 specialists selected to be interviewed, 4 were males and 3 females. Their age range was between 37 to 48 years old. Their expertise includes public sector information security policy makers (3), network and security engineers (2) and public sector security risk supervisors (2). Summary of demographic characteristics in this qualitative data is shown in Table 1. The method of obtaining qualitative data with participants was conducted in an unstructured interview to ensure that participants could provide feedback on information security in public organizations in Malaysia without being bound by any context of the discussion. Therefore,

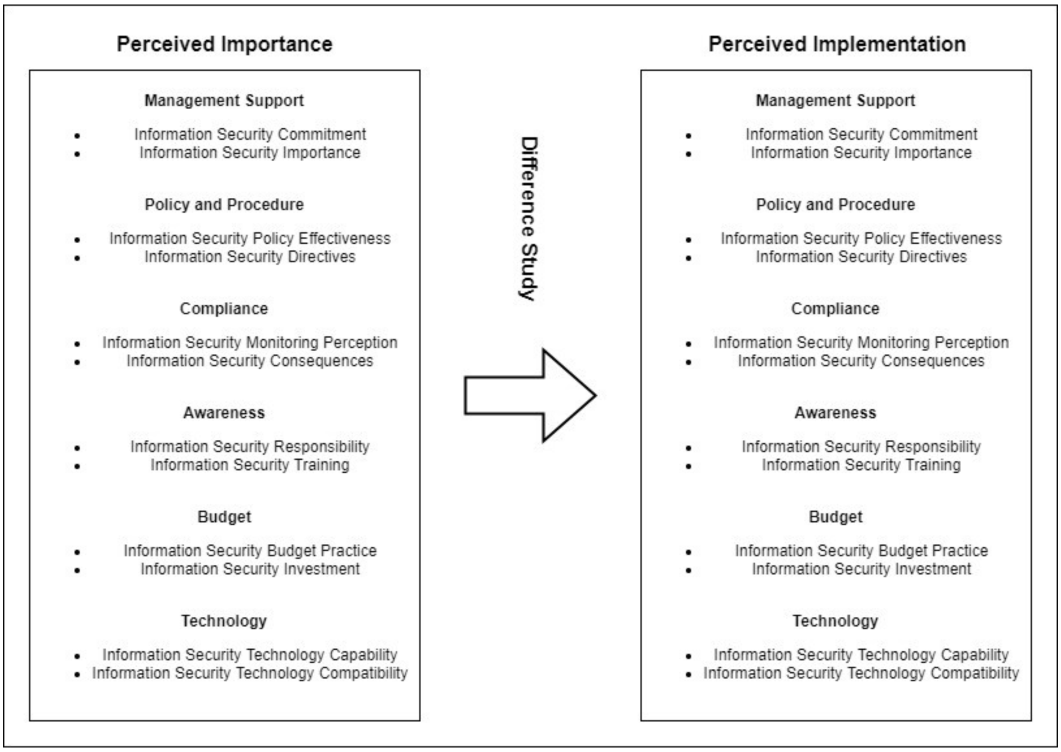
Perceived Importance
Management Support
Information Security Commitment
Information Security Importance
Policy and Procedure
Information Security Policy Effectiveness
Information Security Directives
Compliance
Information Security Monitoring Perception
Information Security Consequences
Awareness
Information Security Responsibility
Information Security Training
Budget
Information Security Budget Practice
Information Security Investment
Technology
Information Security Technology Capability
Information Security Technology Compatibility
Difference Study
Perceived Implementation
Management Support
Information Security Commitment
Information Security Importance
Policy and Procedure
Information Security Policy Effectiveness
Information Security Directives
Compliance
Information Security Monitoring Perception
Information Security Consequences
Awareness
Information Security Responsibility
Information Security Training
Budget
Information Security Budget Practice
Information Security Investment
Technology
Information Security Technology Capability
Information Security Technology Compatibility

Figure 1: Conceptual framework of information security culture

the results of which are given more freely interpreted and further illustrate the reality of information security in the Malaysian public organizations. The interviews were held up to saturated and were seen enough to extract information about information security in public organizations. Each interview session takes about an hour and a half up to two hours. The question that were put forward to the participants were based on the components of the framework. Specifically, the questions asked were:

- Do you think that management support is important for developing ISC? Why?
- Do you think that policy and procedure is important for developing ISC? Why?
- Do you think that compliance is important for developing ISC? Why?
- Do you think that budget is important for developing ISC? Why?
- Do you think that awareness is important for developing ISC? Why
- Do you think that technology is important for developing ISC? Why?

For each of the above questions, further probing were made by asking questions based on the answers given by the participants. For instance, if the participant stated that management support is important, the researcher would further ask why the participant thought that it was important and requested the participant to provide detail elaboration, and if possible cite several instances. The analyses were done by identifying the appropriate themes or category. Similar or common themes were grouped together to form major themes. The common major themes were then grouped together to form the main themes, which we termed as domain of the ISC.

4 Result

In total of 13 themes have been identified related to the qualitative conducted. These themes have been seen consistent with literature studies and have confirmed that element management support

Table 1: Demographic profile of participants

Participants	Expertise	Working Experience (Years)
P1	Network Security	11
P2	Policy Maker	16
P3	Policy Maker	18
P4	Risk Supervisor	23
P5	Policy Maker	18
P6	Risk Supervisor	17
P7	Network Security	13

is one of the crucial ISC dimension to be developed in Malaysia public organization. These are: Management Engagement and Commitment (MEC); Management Attitude (MA); Continuous Monitoring on Policy Compliance (CMPM); Management As Policy Maker (MPM); Mutual Relationship (MR); Employee Performance Evaluating (EPE); Healthy Competition Between Employees (HCE); Job Scope Delivered Well to Employees (JSD); Human Resource Expertise in Safe Guarding The Organization (HRE); Work Ethics (WE); Encouraging to Achieve Objectives (EAO); Continuous Monitoring (CM) and (CE).

4.1 Management Engagement and Committment

The first theme, Management Engagement and Commitment (n = 6), is concerned with the deep involvement and commitment of the top management with information security efforts. This situation is normally manifested through their direct involvement such as being the chairperson of the information security related activities. As the champion of the information security efforts, the top management are expected to provide guidance to their subordinates or employees. These views are shared by P1, P2, P3, P5, P6 and P7 who stated that:

i. "…the most important thing to do is the direct involvement from top management…" (Participant – 1, Code: MEC)

ii. "Top management is supposed to be the foremost person in protecting information from any threats." (Participant – 2, Code: MEC)

iii. "…usually the top management will resolve the issue." (Participant – 3, Code: MEC)

iv. "…the responsibility of the top management is to provide guidance." (Participant – 5, Code: MEC)

v. "…the security aspect should be the most important thing that should be addressed by top management." (Participant – 6, Code: MEC)

vi. "…top management plays a big responsibility to work with employees in protecting organizational information from any threats through consistent security practice until they succeed establishing information security culture." (Participant – 7, Code: MEC)

4.2 Management Attitude

The second theme, Management Attitude (n = 3), is the belief and perception of the top management regarding information security initiatives. A positive attitude by the top management will be translated by their serious attention and commitment to the information security initiatives. This view was put forward by P2:

i. "The seriousness of the attitude shown by top management regarding information security will indirectly alter the attitude of the employees to be more careful in handling organizational information." (Participant – 2, Code: MA)

The positive attitude will also have significant effect on the behavior of the employee. This is because employee will always look and benchmark themselves against the top management in terms of information security practices (P3 and P4).

ii. "Employee will make their top management as a benchmark" (Participant – 3, Code: MA)

iii. "Top management who takes for granted in managing information security will influence employees to also take no serious attention toward information security within the organization" (Participant – 4, Code: MA)

4.3 Continuous Monitoring on Policy Compliance

The third theme, Continuous Monitoring by the Management on Policy Compliance (n = 2), the participants (P1 and P3) expressed their opinion that it is the responsibility of management to ensure that employees comply with prescribed policies and accustomed to performing their duties in the unattended control of the policy, thereby forming information security practices within their organizations, thus reduce the risk of undesirable information security incidents.

i. "...management needs to ensure that the compliance with policies by employees and should be monitored continuously until employees are able to comply with the prescribed policies without being compelled" (Participant – 1, Code: CMPM)

ii. "...management can monitor the continuing compliance of information security policies by all employees to reduce the risk of unwanted incidence" (Participant – 3, Code: CMPM)

4.4 Management as Policy Maker

The fourth theme, Management as Policy Maker (n = 2). As a backbone of the information security practices within Malaysian public organizations, management is responsible for outlining policies on information security as one of their tasks as stated by participants P1 and P2.

i. "...top management is a policy maker..." (Participant – 1, Code: MPM)

ii. "They who draft policies..." (Participant – 2, Code: MPM)

4.5 Mutual Relationship

The fifth theme is Mutual Relationship (n = 3), participant P7 believes that the mutual relationship between management and employees is crucial to build mutual trust that leads to the efficiency of work practices within the organization that contribute to the creation of ISC in Malaysian public organizations.

i. "The relationship between top management and employees plays a big role in creating a safe culture" (Participant – 7, Code: MR)

ii. "I believe that an intimate relationship between top management and employees will make the work in the organization more efficient" (Participant – 7, Code: MR)

iii. "...the most important element in creating information security culture is the relationship between top management and employees..." (Participant – 7, Code: MR)

4.6 Employee Performance Evaluating

The sixth theme is Employee Performance Evaluating (n = 2), participant P2 and P7 expressed their view that monitoring and evaluating employee performance through a balanced scorecard is a good initiative that can be done by the management to ensure that employees are practicing information security practices within the organization.

i. "I strongly agree if governmental organizations can take the initiative to monitor and evaluate employee performance" (Participant – 2, Code: EPE)

ii. "Among the things we can do, by creating a balanced score card to assess employee performance" (Participant – 7, Code: EPE)

4.7 Healthy Competition between Employees

The seventh theme, Healthy Competition between Employees (n = 1), there is an idea raised by the participant P2 where the healthy competition environment created by management can contribute to more effective information security protection, where employees can compete healthily between them to provide balanced protection of information security assets.

i. "Employees in a ministry will be racing to compete with one another in order to be able to compensate for their efforts to safeguard information security effectively" (Participant – 2, Code: HCE)

4.8 Job Scope Delivered Well to Employees

The eighth theme, Job Scope Delivered well to Employees (n = 1), participant P3 is of the view that management is responsible for expressing clearly the scope of work required by employees in the organization. Therefore, employees know what can be done and what should be avoided as stated in the scope of their job, thus creating a safe working practices within their organizations.

i. "…the task and role of each employee in an organization should be clearly defined so that they know what to do and what needs to be kept away…" (Participant – 3, Code: JSD)

4.9 Human Resource Expertise in Safe Guarding the Organization

The ninth theme, Human Resource Expertise in Safe Guarding the Organization (n = 1), participant P5 believes the development of expertise in information security can ensure a secure organizational environment. This is evidenced by the fact of the participant where ministries that have more expertise in technology handling are typically less risk for occurrence of information security threats as compared to ministries lacking expertise in the handling of information security technology.

i. "…any ministry or organization that has the expertise of human resources on technology often does not have much information security incidents compares to ministries or organizations with less expertise in information security aspects…" (Participant – 4, Code: HRE)

ii. "…the task and role of each employee in an organization should be clearly defined so that they know what to do and what needs to be kept away…" (Participant – 3, Code: JSD)

4.10 Work Ethics

The tenth theme, Work Ethics (n = 1), there is a participant (P5) that puts the idea that work ethics is an important thing in the organization that indirectly encourage the employee to practice efficient information security practices and guided by management that is capable of producing a comprehensive ISC.

i. “Work ethics is an important thing. . . ” (Participant – 5, Code: WE)

4.11 Encouraging to Achieve Objectives

The eleventh theme, Encouraging to Achieve Objectives (n = 1), employees need to work diligently to achieve the stated goals and management is responsible to drive rather than forcing employees to achieve organizational objectives. That’s the idea that comes from discussing with a participant (P7) who sees that encouraging to achieve objectives is one of the keys that management should use to build a culture of information security in Malaysian public organizations.

i. “. . . from which we can encourage them to achieve the predetermined objectives rather than punishing them when make mistakes. . . ” (Participant – 7, Code: EAO)

4.12 Continuous Monitoring

The twelfth theme is a Continuous Monitoring (n = 3), a participant (P1) emphasizes that ISC seedling should be monitored continuously until it succeeds in enhancing this particular culture in Malaysian public organization.

i. “. . . there must be continuous monitoring until succeed establishing culture. . . ” (Participant – 1, Code: CM)

Participants P3 and P4 add every action related to the protection of information assets and incident management should be reported in the daily log as one of the education of employees to do what is right to become a culture practiced within the organization.

ii. “. . . employees need to report every action on the protection of information assets and incident management on daily logs. . . ” (Participant – 3, Code: CM)

iii. “This surveillance is aimed at educating employees to do what is right until the practice becomes a culture within the organization” (Participant – 4, Code: CM)

4.13 A Continuous Effort to Build Safe Culture

The thirteen theme, Continuing Efforts to Build Safe Culture (n = 2), (P2) participant argue that providing ongoing guidance plays a big role in educating employees so that general knowledge about information security threats is understood by employees in the organization and at intervals, it will be a very mature safe culture practiced by everyone within the organization across positions and levels.

i. “. . . provide continuous guidance until employees are well aware of the importance and can safeguard information assets. . . ” (Participant – 2, Code: CE)

ii. “Over time, efforts to protect the safety of this information will be a work culture within the organization.” (Participant – 2, Code: CE)

5 Discussion

Organizational leadership plays an important role to ensure the organization is fenced off by a “security wall” or more precisely the “human firewall” that can prevent the organization’s information assets from the next generation of cyber-attack. Organization’s well-being in terms of confidentiality, integrity and availability can be threatened through various incidents caused by either from internal or external sources. In the Malaysian context, this study has found that management plays a very important role in nurturing ISC among employees. As mentioned in the previous section, the themes that have been identified show that the management support element is the most important element that can be lifted as the main dimension in the ISC model of Malaysian public organization. Fagerstrom's (2013) (Fagerstrom, 2013) also supports that the development of ISC should start with top management as the most important layer in the organization. Gaunt (2002) Gaunt et al., 2002 added that, to establish long-term success of resilient information security, strong leadership in top management are crucial and indispensable in the early stages. Additionally, Figure 2 illustrates the themes obtained in this study. For future studies, researchers may consider using these themes to develop a dimension that focuses more specifically on leadership and management aspects of ISCs and can be applied in different settings whether government, private or MSC titled organizations.

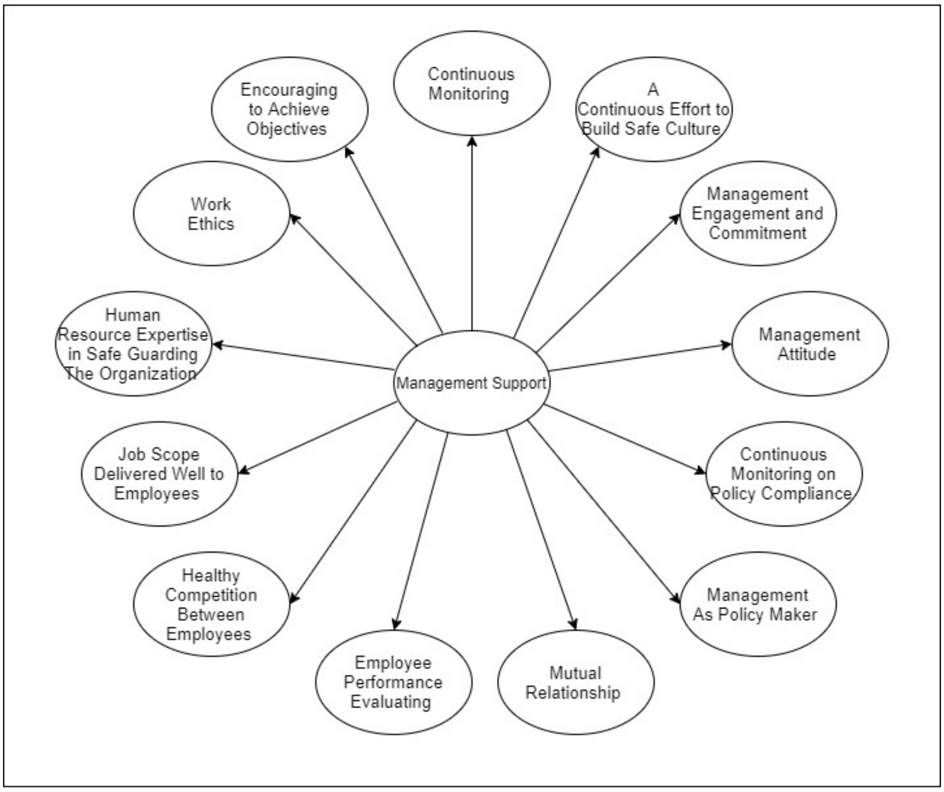
Management Support
Continuous Monitoring
Encouraging to Achieve Objectives
A Continuous Effort to Build Safe Culture
Work Ethics
Management Engagement and Commitment
Human Resource Expertise in Safe Guarding The Organization
Management Attitude
Job Scope Delivered Well to Employees
Continuous Monitoring on Policy Compliance
Healthy Competition Between Employees
Management As Policy Maker
Employee Performance Evaluating
Mutual Relationship

Figure 2: Management support theme in information security culture

6 Conclusion

This study demonstrates that management support is one of the most important factor to instil ISC in Malaysia public organization. Organizational leadership should play a holistic role to ensure the establishment of a strong and solid ISC within the organization. Among the things that can be done is to demonstrate commitment with every activity that is done with the employee in order to build mutual respect and strong relationship between employees and management. Furthermore, by showing enthusiasm for the importance of information security within the organization, management can influence the behaviour of employees to work together to create a safe working environment. As the forefront of the organization, management can also develop security policies that can be complied with and well communicated to all employees, thus monitoring employees' compliance with established policies. For workers who are less concerned about the importance of information security, management can provide encouragement in the form of incentives to outstanding employees in terms of compliance with information security policy. Indirectly create healthy competition among employees to protect information security, and achieve organizational objectives.

Acknowledgment

The researcher would like to extend our thanks and appreciation to Universiti Teknologi MARA (UiTM) and the Ministry of Higher Education (MoHE) Malaysia for funding the project under the Fundamental Research Grant Scheme, file no: FRGS/1/2016/SS09/UITM/02/2.

References

A, A. and M, P. (2018). Personal details of over 200,000 malaysian organ donors leaked online: report.

Allen, B. (1968). Danger ahead-safeguard your computer. *Harvard Business Review*, 46(6):97–101.

Ar, Z. (2018). Putrajaya's exam portal shut down, after data breach affecting millions: Malay mail.

Beaver, K. (2015). The importance of a security culture across the organization. *Secur ityintelligence. com. https://securityintelligence. com/the-importance-of-a-security- culture-across-the-organization*.

ENISA (2018). Cybersecurity culture guidelines: behavioural aspects of cybersecurity.

Fagerstrom, A. (2013). Creating, maintaining and managing an information security culture. Master's thesis, Bradenburg University of Technology, Cottbus, Senftenberg, Germany.

Gaunt, R., Leyens, J.-P., and Demoulin, S. (2002). Intergroup relations and the attribution of emotions: control over memory for secondary emotions associated with the ingroup and outgroup. *Journal of Experimental Social Psychology*, 38(5):508–514.

Knapp, K. J., Franklin Morris, R., Marshall, T. E., and Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, 28(7):493–508.

Mahfuth, A., Yussof, S., Baker, A. A., and Ali, N. (2017). A systematic literature review: Information security culture. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, pages 1–6.

Masrek, M., Harun, Q., and Sahid, N. (2018). Assessing the information security culture in a government context: the case of a developing country. *International Journal of Civil Engineering and Technology*, 9(8):96–112.

MyCERT (2020). Mycert.

Parker, D. B. and Gardetto, B. J. (1981). *Computer security management*. Reston Publishing Company.

Romeo, C. (2021). 6 ways to develop a security culture in your organization.

Straub, D. W. (1990). Effective is security: An empirical study. *Information Systems Research*, 1(3):255–276.

Tassel, D. V. (1972). *Computer Security Management*. Prentice-Hall.

2021 ICMS

INTERNATIONAL CONFERENCE ON COMPUTING,
MATHEMATICS AND STATISTICS

e ISBN 978-967-2948-12-4

9 7 8 9 6 7 2 9 4 8 1 2 4