Journal of Engineering & Technological Advances ISSN: 2550-1437
Vol. 1, No 1, 2016

FACILITATING THE INVESTIGATION OF INFORMATION SECURITY CASES BY USING EVALUATION MATRIX

Norriza Hussin[1*]
[1]School of Information Technology, SEGi University, Malaysia
*Email: norriza@segi.edu.my

ABSTRACT

This paper intends to propose the construction of an evaluation matrix as a tool to facilitate the investigation of information security cases. In this paper, the components of the evaluation matrix are introduced and explained. This paper has been divided into four different parts. The first part explains the background information on information security in Malaysia while the research questions will be explained in the second part of the paper. The paper continues to illustrate the origins of the proposed evaluation matrix in part three. The final part embraces the importance of using the evaluation matrix to facilitate the existing method in the investigation of information security cases.

Keywords: *Information security, information reliability, investigation, evaluation matrix, competency criteria.*

1.0 INFORMATION SECURITY

New technologies have instigated cyber security threats. Based on a Report by Cyber Security Malaysia, a total of out of 99,986 incidents have been reported to their organization in 2012 with intrusion and fraud making up eighty-three percent of the total number of incidents.

CyberSecurity Malaysia was launched in 2007 (CyberSecurity, n.d.) and the organization was formerly known as the National ICT Security & Emergency Response Centre (NISER). One of the tasks carried out by CyberSecurity Malaysia is to develop information security guidelines for the general public with a view to assist them in operating in a secured information security environment.

The "Guideline to Determine Information Security Professionals Requirements for the Critical National Information Infrastructure (CNII) Agencies/Organizations" (CyberSecurity, 2012) will be referred to as "the Guideline" throughout this paper. In the foreword of the Guideline, it has been stated that cyber-attacks have become a serious concern. The publication of the Guideline was stemmed through the decision made in the National Cyber Crisis Management Meeting (NCCMC) in the year 2012 deliberating the significance of having qualified information security professionals in the Critical National Information Infrastructure (CNII).

Section 5 of the Guideline defines the competency criteria for Information Security Operations, Information Security Compliance and Information Security Audit.

This paper concentrates on Section 5 of the Guideline which focuses on the Information Security Incident Management. It has been further stated in the Guideline that:

> "Relevant knowledge and experience in incident management, forensics investigations and preservation of date including:
> - Information security incident reporting
> - Collecting and preservation of digital evidence
> - Information security incident root cause analysis
> - Corrective and preventive action for continual improvement".

This study envisages the similarities of the incident management guideline with the second part of the evaluation matrix.

2.0 RESEARCH QUESTIONS

This paper proposes two research questions pertaining to the evaluation matrix:

a) How are the skills and experience of the investigators being reflected on the investigations?
b) How can the certainty factors from the evaluation matrix be used as a tool to assess the reliability of the investigation based on the following aspects; qualifications, experience, accuracy, appropriacy, satisfaction and reliability.

The study aims to establish the relevance of the evaluation matrix in assessing the validity and certainty of the investigation procedures.

3.0 EVALUATION MATRIX

The evaluation matrix originated from a research on evidential analysis (Hussin, 2014). The matrix (Library, Human Intelligence Collector Operation, 2006) has been divided into two parts (Hussin, Evidential Analysis for Computer-Generated Animation (CGA), 2006) whereby the first part focuses on the information security professionals with the following aspects:

a) Competence. An example of competence is when an individual displays competence, the interpretation is, that he or she knows how.
b) Acquaintance. An example of acquaintance is when an individual may be said to know that with which he or she is acquainted. When a person knows something, in this sense, is to say that he/she has had some experience with what he/she knows.
c) Recognition of information as being correct. This is knowledge in the (correct) “information” sense. When a person recognizes correct information as being correct.

The second part of the matrix interrelates the working method with the professionals. The working method with regard to this study refers to the investigation process of the information

security cases and the following aspects are highlighted in the second part of the matrix (Schofield D., 2005):

a) That the information p be correct. The first condition is that information p be true. S knows the information p.
b) That S accepts the information p. In order to recognize information as correct is to have an attitude toward it. The knower S endorses the information in the sense that S stands behind it or endorses it as being correct. Another way to describe the endorsement is to say that S thinks that p is correct or true information.
c) That the acceptance of the information that p be justified. In this regard, is to determine that justification lies between reasonableness and complete certainty.

References to the components have been made as follows:

(1)	K1	Professionals
	K1a	Competence
	K1b	Acquainted
	K1c	Recognition
(2)	K2	Method
	K2a	Truth
	K2b	Acceptance
	K2c	Justification

The letter "K" has been chosen based on the word "knowledge" as the components originates from the basic principles of the Theory of Knowledge (Lehrer, 1990). The components in K1 and K2 will then be elaborated under the following three categories:

(1) General: relates to the general conditions of the components.
(2) Similar: relates to the similar conditions of the components.
(3) Exact: relates to the exact conditions of the components.

The evaluation matrix will be developed in the near future as a proposed tools in facilitating the investigation of information security cases.

4.0 THE IMPORTANCE OF THE EVALUATION MATRIX AS A TOOL

Further evaluation on each of the criteria listed in the Guideline (CyberSecurity, n.d.) with the description in the evaluation matrix could be performed in the future. This method would be advantageous to the organization involved in information security investigation in terms of competency and reliability.

The main objective of the evaluation matrix is to assist the process in verifying correct and accurate information in relation to cases under investigation (Hussin N., 2004).

Skills and experience of the investigators are important to ensure the validity and accuracy of the investigation. In addition, the working methods hold the same weight in determining a particular level of certainty in the investigation. The author anticipates a development of the evaluation matrix for future work. In addition to the development, the evaluation matrix has potential to be elaborated based on the impending issues arising during the process of investigation. The author envisages that literature and preliminary work on software development would be incorporated to offer a multi-disciplinary research within this topic.

5.0 REFERENCES

- CyberSecurity. (2012). *Guideline to Determine Information Security Professionals Requirements for the Critical National Information Infrastructure (CNII) Agencies/Organisations.* Retrieved July 28, 2016, from Guideline to Determine Information Security Professionals Requirements for the Critical National Information Infrastructure (CNII) Agencies/Organisations
- CyberSecurity (n.d.). *Guideline to Determine Information Security Professionals Requirements for the Critical National Information Infrastructure (CNII) Agencies/Organisations.* http://www.cybersecurity.my/data/content_files/11/1159.pdf?.diff=1373447691
- Hussin, N. (2006). *Evidential Analysis for Computer-Generated Animation (CGA).* University of Nottingham.
- Hussin, N. (2014). Evaluation Matrix: Information Security Investigation in Malaysia. *5th International Workshop on Computer Science and Engineering (WCSE) 2015* (pp. 796-802). Moscow: The SCIence and Engineering Institute.
- Hussin, N. Schofield D., Shalaby M.T. (2004). Visualising Information: Evidence Analysis for Computer-Generated Animation (CGA). *Proceedings of the Eighth International Conference on Information Visualisation* (pp. 903-908). IEEE Computer Society.
- Lehrer, K. (1990). *Theory of Knowledge.* Westview Press, Inc.
- Library, P. (2006). *Human Intelligence Collector Operations.* Human Intelligence Collector Operations, 3rd ed., Pentagon Library, Military Documents, Washington, DC20310, 2006. http://books.google.com.my/books?id=c6mp5QHkJ8YC&pg=PT4&dq=intelligence+source+reliability+a1&lr=&num=50&as_brr=3&cd=3&redir_esc=y#v=onepage&q&f=false
- Schofield D., Hussin N., Shalaby M.T. (2005). A Methodology for Evidential Analysis for Computer-Generated Animation (CGA). *IV '05 Proceedings of the Ninth International Conference on Information Visualisation* (pp. 565-570). Washington: IEEE Computer Society.