2015 The 5th International Workshop on Computer Science and Engineering
doi: 10.18178/wcse.2015.04.127

Evaluation Matrix: Information Security Investigation in Malaysia

Norriza Hussin

School of Information Technology, SEGi University, Malaysia

norriza@segi.edu.my

Keywords: Information Security; Information Reliability; Investigation; Evaluation Matrix.

Abstract. This paper aims to propose an evaluation matrix for the purpose of investigation on information security cases. The origin of the evaluation matrix has been derived from the research undertaken in the University of Nottingham (Hussin, 2006). The author envisages that a research on information reliability would substantiate the investigation for information security cases in Malaysia. Based on the existing investigation procedure, this paper intends to propose an evaluation matrix to support the current process. The evaluation matrix measures and assesses the skills and expertise of the investigators.

Introduction

Threats to information and information systems may be categorised and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: *confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability*." (Cherdantseva and Hilton, 2013).

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

Inter-Connecting the Core Element

Current Issues This paper realizes the importance of correct and accurate information to be delivered before, during and after the investigation. The author intends to corroborate the proposed evaluation matrix into the current investigation process in the information security cases in Malaysia. The function of the evaluation matrix is to assist in determining the qualities of skills and expertise. The qualities which embraces the following: (a) appropriate; (b) satisfactory; and (c) reliable will be further explained in Section Proposed Evaluation Matrix.

Significance In Figure 1, the main element is information reliability. In this paper, conditions for knowledge are the core content for information reliability.

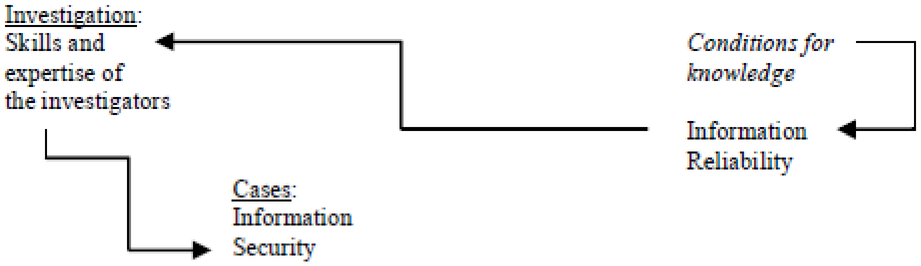

Figure 1 Inter-connecting the core elements.

The inter-connection that has been illustrated in Figure 1 further describes that information reliability has been proposed to be an eminent aspect to be corroborated in the investigation process of information security cases. The skills and expertise of the investigators that satisfy the proposed evaluation matrix would be essential to ensure the efficiency on how information are being managed, used and evaluated throughout the investigation.

The main objective of the evaluation matrix is to assist the process in verifying correct and accurate information on the cases under investigation. This paper proposes a number of research issues pertaining to the evaluation matrix:

- How the skills and experience of the investigators reflect on the investigation?
- How can the conditions for knowledge be applied into the evaluation matrix to corroborate the current procedure in the investigation on cases involving information security?

In addition to the main objective, the paper aims to propose that the evaluation matrix could be use to achieve a level of certainty in determining as to whether the expert and skills are reliable to undertake the investigation.

Information Reliability

In this paper information reliability has been described into two segments. Segment no. 1 refers to the types of knowledge (Lehrer, 2002):

- Competence. An example of competence is when an individual displays competence, the interpretation is, that he or she knows how.
- Acquaintance. An example of acquaintance is when an individual may be said to know that with which he or she is acquainted. To say that one knows something, in this sense, is to say that they have had some experience with what they know.
- Recognition of information as being correct. This is knowledge in the (correct) “information” sense. To know is to recognize correct information as being correct.

Further by Lehrer (2000), Segment no. 2 refers to the *S* and *p* as variables for the conditions for knowledge. *S* represents any information that can be known:

- That the information *p* be correct. The first condition is that information *p* be true. *S* knows the information *p*.
- That *S* accepts the information *p*. 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.
- That the acceptance of the information that *p* be justified. To determine that justification lies between reasonableness and complete certainty.

For the purpose of this paper, types of knowledge and conditions for knowledge will be referenced as K1 and K2 as shown in Table 1.

Table 1: Referencing Segments no. 1 and no. 2.

K1	Types of knowledge
K1a	Competence
K1b	Acquaintance
K1c	Recognition of information as being correct
K2	Conditions for knowledge
K2a	Truth
K2b	Acceptance
K2c	Justification

Proposed Evaluation Matrix

The importance of information reliability has been further elaborated in this paper by Table 2. The certainty factors focuses on the skills and expertise in a particular area. In this paper, the area is IP. The following factors from both segments are being proposed into the evaluation matrix:

- qualification and training (K1a: competence);
- work related experience (K1b: acquaintance);
- accuracy (K1c; correct information)
- appropriate (K2a: truth);
- satisfactory (K2b: acceptance); and
- reliable (K2c: justification)

K1a and K1b have been referred to the expert’s academic, training and experience background. Whilst, K1c refers to the accuracy of the information gathered and managed by the expert.

K2a, K2b and K2c have been referred to the specific rules or process applied to the work process. For example, the identification and verification process in the investigation.

Table 2: Detailed certainty factors based on conditions for knowledge (Hussin, 2006).

Part I

K1a	0.1 0.2 0.3	obtained qualification and training on general investigation process
	0.4 0.5 0.6	obtained qualification and training to a similar case
	0.7 0.8 0.9 1.0	obtained qualification and training on exactly the same type of case under investigation
K1b	0.1 0.2 0.3	acquired previous experience on general investigation process
	0.4 0.5 0.6	acquired previous experience pertaining to a similar case
	0.7 0.8 0.9 1.0	acquired previous experience on exactly the same type of case under investigation
K1c	0.1 0.2 0.3	obtained general information
	0.4 0.5 0.6	obtained information from a third party
	0.7 0.8 0.9 1.0	obtained information directly from the source

Part II

K2a	0.1 0.2 0.3	applied a scientific/specific rule based on experience, training and qualification for other types of case.
	0.4 0.5 0.6	applied a scientific/specific rule based on experience, training and qualification for a similar types of case.

	0.7 0.8 0.9 1.0	applied a scientific/specific rule based on experience, training and qualification for the case under investigation.
K2b	0.1 0.2 0.3	ability to endorse the scientific/specific rule based on experience, training and qualification for other types of case.
	0.4 0.5 0.6	ability to endorse the scientific/specific rule based on experience, training and qualification for a similar types of case.
	0.7 0.8 0.9 1.0	ability to endorse the scientific/specific rule based on experience, training and qualification for the case under investigation.
K2c	0.1 0.2 0.3	ability to validate the scientific/specific rule based on experience, training and qualification for other types of case.
	0.4 0.5 0.6	ability to validate the scientific/specific rule based on experience, training and qualification for a similar types of case.
	0.7 0.8 0.9 1.0	ability to validate the scientific/specific rule based on experience, training and qualification for the case under investigation.

Conclusions

The importance of information reliability would be the essence to ensure that the quality of the investigation can be measured for integrity and accountability. A similar matrix has been implied in evidential analysis for computer-generated animation (Hussin, 2006). The author is proposing further research on developing the evaluation matrix. The evaluation matrix would benefit the process of the investigation by assigning the competent, skilled, and experienced investigators to undertake the investigation tasks.

Acknowledgements

The author would like to thank SEGi University Malaysia for the support and encouragement.

References

[1] Cherdantseva Y. and Hilton J.: Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals In: Organisational, Legal and Technological Dimensions of Information System Administrator. Almeida F. Porteak. I. (eds.) IGI Global Publishing. (2013).

[2] Bayuk, Jennifer. Understanding Information Security Investigation. Spinger's Forensic Laboratory Science Series. 2010.

[3] CyberSecurity Malaysia. http://www.cybersecurity.my/en/index.html (Date last accessed: 7/9/2014).

[4] *Human Intelligence Collector Operations,* 3rd ed., Pentagon Library, Military Documents, Washington, DC20310, 2006. Available at

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 (Date last accessed: 7/9/2014).

[5] Hussin, N., Schofield, D. and Shalaby, M. T., “Visualising Information: Evidence Analysis for Computer-Generated Animation (CGA)”, *Proceedings of 8th International Conference on Information Visualisation IV04, London, 14-16th July, 2004*.

[6] Hussin, N. “Evidential Analysis for Computer-Generated Animation (CGA),” Ph.D. dissertation, School of Computer Science and IT, University of Nottingham, U.K. 2006.

[7] Shalaby, M. T.; Hussin, N.; and Schofield; D. “Forensic Animation: Measuring the Reliability and Accuracy of Computer Generated Animation Used in the Courtroom”, *Proceedings of the 7th International Conference on Information Visualisation IV03, London, 16-18th July 2003*.

[8] Schofield, D., Hussin, N. and Shalaby, M. T., “A Methodology for Evidential Analysis for Computer-Generated Animation (CGA)”, *Proceedings of 9th International Conference on Information Visualisation IV05, London, 6-8th July, 2005*.