Malaysia Technical Scientist Association
Registration No: PPM-009-04-12012015

LECTURE NOTES IN COMMUNICATION AND COMPUTER ENGINEERING

Editors:
Hamzah Asyrani Sulaiman
Mohd Azlishah Othman
Mohd Shakir Md Saat
Abd Majid Darsono
Ahmad Naim Che Pee
Mohd Fairuz Iskandar Othman
Yahaya Abd Rahim
Mai Mariam Mohamed Aminuddin
Mohamad Harris Misran

Lecture Notes in Communication and Computer Engineering
eISBN: 978-967-2348-14-6

Published in Malaysia by:
Malaysia Technical Scientist Association
No 47, Jalan TU 25, Taman Tasik Utama,
75450 Ayer Keroh, Melaka, Malaysia
E-mail: admin@maltesas.my

PREFACE

This e-book presents selected papers from the 5th International Conference on Communication and Computer Engineering 2018, that was conducted from 17th to 19th July 2018 in Melaka, Malaysia. It is an international forum for researchers, academics and practitioners to present their work, to formulate new challenges and to discuss current state-of-the-art technology in computer networking, computer engineering and communication technology. This e-book will serve as a valuable reference resource for academics and researchers across the globe.

WELCOME MESSAGE

It was gratifying to all of us when the response for ICOCOE'18 is overwhelming as the technical committees received more than 100 submissions from various areas of communication and computer engineering. All submitted papers are then peer-reviewed, revised according to the reviewers' comments and ultimately 48 papers were accepted for publication in this e-book.

This open access e-book can be viewed or downloaded via **https://maltesas.my/msys/explore**. We hope that this e-book will serve as a valuable reference for researchers.

As the Editor-in-Chief, I would like to express our gratitude to the fellow review members for their effort in reviewing the submitted papers for this e-book. I also would like to say special thanks to all the authors for promptly revising their papers according to the requirements.

Thank you.

Mohd Azlishah Othman
Editor-in-Chief

EDITORIAL COMMITTEE

Azuwa Ali - Universiti Malaysia Perlis, Malaysia

Baichuan Zhang - Purdue University, USA

Bayu Adhi Tama - Ulsan National Institute of Science and Technology (UNIST), Korea

Benoît Muth - Benoît Muth, France

Boon Chong Ang - Intel, Malaysia

Carlos Travieso - University of Las Palmas de Gran Canaria, Spain

Chakree Teekapakvisit - King Mongkut's Institute of Technology Ladkrabang, Thailand

Chau Yuen - Singapore University of Technology and Design, Singapore

Chien-Jen Wang - National University of Tainan, Taiwan

Chutisant Kerdvibulvech - National Institute of Development Administration, Thailand

Dan Ciulin - E-I-A, Switzerland

Dan Milici - University of Suceava, Romania

Deepak Choudhary - LPU, India

Dhananjay Singh - Hankuk University of Foreign Studies, Korea

Dinesh Bhatia - Biomedical Engineering Department, North Eastern Hill University, India

Dirman Hanafi - Universiti Tun Hussein Onn Malaysia, Malaysia

Domenico Ciuonzo - Network Measurement and Monitoring (NM2), Naples, IT, Italy

Domenico Rotondi - FINCONS SpA, Italy

Dragana Krstić - Faculty of Electronic Engineering, University of Niš, Serbia

Eduard Babulak - Fort Hays State University, USA

Eduardo Pinos - Universidad Politécnica Salesiana, Ecuador

Eliana Werbin - Universidad Nacional de Cordoba, Argentina

Emilio Jiménez Macías - University of La Rioja, Spain

Fairul Azhar Abdul Shukor - Universiti Teknikal Malaysia Melaka, Malaysia

Fei Qin - Chinese Academy of Sciences, P.R. China

George Tambouratzis - Institute for Language & Speech Processing, Greece

George Suciu - Politehnica University of Bucharest, Romania

Ghulam Abbas - GIK Institute of Engineering Sciences & Technology, Pakistan

Giovanni Palmerini - Università di Roma La Sapienza, Italy

Giuseppe Lo Re - University of Palermo, Italy

Go Yun Il - Heriot-Watt University Malaysia, Malaysia

Haijun Pan - New Jersey Institute of Technology, USA

Hamidah Ibrahim - Universiti Putra Malaysia, Malaysia

Harikumar Rajaguru - anna University Chennai, India

Hasimah Mohamed - Universiti Sains Malaysia, Malaysia

Hua Nong Ting - Universiti Malaya, Malaysia

Hyunbum Kim - University of North Carolina at Wilmington, USA

Ida Laila Ahmad - Universiti Tun Hussein Onn Malaysia, Malaysia

Iman Sharifi - Amirkabir University of Technology, Iran

Ishak Annuar - Universiti Teknologi MARA (UiTM) Kota Samarahan Sarawak, Malaysia

Jason Zurawski - Energy Sciences Network, USA

Jiachyi Wu - National Taiwan Ocean University, Taiwan

Jonathan de Silva - Instituto Nacional de Telecomunicações, Brazil

Josip Music - University of Split, Croatia

Jouni Tervonen - University of Oulu, Finland

Juan Durillo - Leibniz Supercomputing Centre, Germany

K Mahantesh - SJBIT, India

Karim Al-Saedi - Mustansiriyah University, Iraq

Katerina Kabassi - TEI of the Ionian Islands, Greece

Kia Hock Tan - Universiti Tunku Abdul Rahman, Malaysia

Kira Kastell - Frankfurt University of Applied Sciences, Germany

Krishna Battula - Jawaharlal Nehru Technological University Kakinada, India

Leonardo Ramirez - Universidad Militar de Nueva Granada, Colombia

Li Wah Thong - Multimedia University, Malaysia

Lien-Wu Chen - Feng Chia University, Taiwan

Lyes Khoukhi - University of Technology of Troyes, France

Maged Marghany - Universiti Teknologi Malaysia, Malaysia

Mahdi Karami - Universiti Putra Malaysia, Malaysia

Mahmoud Rokaya - Taif University, Saudi Arabia

Mariusz Zal - Poznan University of Technology, Poland

Martin Neumann - Karlsruhe Institut of Technology (KIT), Germany

Martine Wedlake - Amazon, USA

Ming-Fong Tsai - National United University, Taiwan

Mohamad Misran - Universiti Tenikal Malaysia Melaka, Malaysia

Mohamed Najeh Lakhoua - SMS, ENICarthage, Tunisia

Mohammad Faiz Liew Abdullah - Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia

Mohammad Rakib Uddin - UniversitiTeknologi Brunei, Brunei Darussalam

Mohd Alif - Universiti Malaysia Perlis, Malaysia

Mohd Khanapiah Nor - Universiti Teknikal Malaysia Melaka, Malaysia

Mohd Najib Mohd Yasin - Universiti Malaysia Perlis, Malaysia

Montree Kumngern - King Mongkut's Institute of Technology Ladkrabang, Thailand

Muhammad Ayoub - Universiti Teknologi PETRONAS, Malaysia

Muhammad Johal - Universiti Teknikal Malaysia Melaka, Malaysia

Muhammad Anshar - Hasanuddin University, Indonesia

Muhammad Hafidz Fazli Bin Md Fauadi - Universiti Teknikal Malaysia Melaka, Malaysia

Muhammad Mokhzaini Azizan - Universiti Malaysia Perlis, Malaysia

Muhammad Reza Kahar Aziz - Institut Teknologi Sumatera, Indonesia

Muharrem Tümçakır - Aselsan Inc. Defense Systems Technologies Division, Turkey

Nadheer Shalash - Al-Mamon University College, Iraq

Nasser Mohamed Ramli - Universiti Teknologi PETRONAS, Malaysia

Nishant Doshi - PDPU, India

Nooririnah Omar - Universiti Technical Malaysia Malacca (UTeM), Malaysia

Norazah Mohd Suki - Universiti Malaysia Sabah, Malaysia

Noriko Etani - Peach Aviation Limited, Japan

Nurbahirah Norddin - Universiti Teknikal Malaysia Melaka, Malaysia

Omar Farooq - Aligarh Muslim University, Aligarh, India

Pablo Corral - Miguel Hernández University, Spain

Paolo Crippa - Università Politecnica delle Marche, Italy

Philip Moore - Lanzhou University, P.R. China

Pingyi Fan - Tsinghua University, P.R. China

Pooya Taheri - SFU, Canada

Rachit Patel - ABESIT Engineering College, Ghaziabad, India

Radu Vasiu - Politehnica University of Timisoara, Romania

Ramesh Kumar Ayyasamy - Universiti Tunku Abdul Rahman (UTAR), Malaysia

Ravi Subban - Pondicherry University, Pondicherry, India

Rijalul Fahmi Mustapa - Universiti Teknologi MARA, Malaysia

Robert Szabolcsi - Óbuda University, Hungary

Rong Nan Chiou - Southern Taiwan University, Taiwan

Rosaura Palma-Orozco - Instituto Politécnico Nacional, Mexico

Rostam Affendi Hamzah - Universiti Teknikal Malaysia Melaka, Malaysia

Rostyslav Sklyar - Independent Professional, Ukraine

Sallehuddin Ibrahim - Universiti Teknologi Malaysia, Malaysia

Salman Yussof - Universiti Tenaga Nasional, Malaysia

Samsul Ariffin Abdul Karim - Universiti Teknologi Petronas, Malaysia

Sangheethaa Sukumaran - dilla University, Ethiopia

Selva Perumal Sathish Kumar - Asia Pacific University of Technology and Innovation, Malaysia

Shahid Manzoor - UCSI Universiti Kuala Lumpur, Malaysia

Shashikant Patil - SVKM NMIMS Mumbai India, India

Siamack Ghadimi - Western University, Canada

Sin Liang Lim - Multimedia University, Malaysia

Siti Aslina Hussain - Universiti Putra Malaysia, Malaysia

Smain Femmam - University UHA, France

Sreedharan Pillai Sreelal - Indian Space Research Organization, India

Srinivasulu Tadisetty - Kakatiya University College of Engineering and Technology, India

Su Fong Chien - MIMOS Berhad, Malaysia

Sulaiman Wadi Harun - Uni Malaya, Malaysia

Su-Lim Tan - Singapore Institute of Technology, Singapore

Susanna Spinsante - Università Politecnica delle Marche, Italy

Teddy Gunawan - International Islamic University Malaysia, Malaysia

Thaweesak Yingthawornsuk - King Mongkut's University of Technology Thonburi, Thailand

Thiang Hwang Liong Hoat - Petra Christian University, Indonesia

Thy Ling - UCTS, Malaysia

Tomonobu Senjyu - Faculty of Engneering, University of the Ryukyus, Japan

Toshiaki Koike-Akino - Mitsubishi Electric Research Laboratories (MERL), USA

Tun Zainal Azni Zulkifli - Universiti Teknologi PETRONAS, Malaysia

Vinesh Thiruchelvam - Asia Pacific University (APU), Malaysia

Vitor Cunha - Instituto de Telecomunicações, Portugal

Waail Al-waely - Griffith University / School of Engineering, Australia

Wael Salah - Palestine Technical University - Kadoorie, Palestine

Wei Wei - Xi'an University of Technology, P.R. China

Yaareb Al-Khashab - Ministry of Water Resources/Badush Dam, Iraq

Yi Zhang - Trinity College Dublin, Ireland

Yilun Shang - Northumbria University, United Kingdom

Yingmeng Xiang - GEIRI North America, USA

Yogesh Pundlik - Kamala Institute of Technology and Science, Singapur-, India

Zahéra Mekkioui - University of tlemcen, Algeria

Zoubir Mammeri - Paul Sabatier University, France

TABLE OF CONTENTS

Model of Risk Estimation using Multiple Criteria of Business Perspective

Prajna Deshanta Ibnugraha[1, 2], Lukito Edi Nugroho[1], Paulus Insap Santosa[1]
[1]*Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Yogyakarta, Indonesia*
[2]*School of Applied Science, Telkom University, Bandung, Indonesia.*
prajna.deshanta.i@mail.ugm.ac.id

***Abstract*—Currently, digital information is essential asset for supporting business of enterprises where it can be categorized as sensitive information and public information. However, security threat of sensitive information causes incident that it has impact to business of enterprises. Therefore, information security becomes important element where it must be applied to protect sensitive information from illegal access. However, analysis of threat and risk must be performed before implementing protection method for sensitive information. In order to analyze threat and risk, enterprises need risk model as a reference where it must consider priority of business aspects. Several existing models actually have included business aspects, but they still need development related priority feature of aspects. Therefore, this study has objective to develop risk estimation model where it involves priority of business aspects to result risk profile. In order to reach objective, this study uses Analytic Hierarchy Process (AHP) as weighting method. Experimental part in this study results weight of metrics where they have different portion. Weight of metrics is tested to two different enterprises to measure value of risk. In experimental condition, both of enterprises have same threat of information security. Output of testing indicates that two different characteristic of enterprises result two different level of risk eventhough they have same type of threat. The high value of information security threat in risk estimation process indicates that threat has high priority of risk. If enterprise has high priority of threat then enterprise must give more concern in mitigation solution to that threat.**

***Index Terms*—business aspects; information security; multiple criteria; risk estimation.**

I. INTRODUCTION

Nowadays, information technology is an essential component in business of enterprises. Implementation of information technology has reached in almost all sectors of enterprises business such as marketing, finance, operations, etc. Implementation of information technology in enterprises generally involves assets such as infrastructure, services, software and information. Some assets have critical category where it has high impact to business of enterprises. Therefore, enterprises need to consider security aspects to protect critical assets. In context of information asset, enterprises need to perform security assessment. Security assessment is a process for evaluating information security by looking at the threats and impacts. The output of the security assessment is used as input for the company to formulate policies related mitigation procedures.

In order to determine impact of information security threats, enterprises need risk model [1]. Several risk models commonly used by enterprises are Common Vulnerability Score System (CVSS), The Open Web Application Security Project (OWASP) and DREAD. However, risk models above have limitations regarding business approach and priority feature. In DREAD model, business perspectives are less involved as determining metrics [2]. Business approach has been involved in OWASP metrics, but it does not have priority. OWASP uses equal weight for measuring impact of information security threat [3]. In CVSS model, weighting has been implemented on its metrics. However, CVSS model has high complexity and implicit metrics to represent business perspectives [4].

Limitation in priority feature and business approach in metrics of risk model becomes important issues where it needs to be resolved to accommodate the need of enterprises related risk model. Therefore, this paper aims to develop risk model where it considers priority options and business approach.

II. RELATED WORK

Studies of risk model in security of information technology had been conducted and published by the researchers. Ghani et al. studied model of risk estimation with quantitative approach where it referred to economic-driven [5]. Ghani et al. used Multiplicative Analytic Hierarchy Process (MAHP) as method and involved some metrics like Reputation Loss, Investor Loss, Customer Loss and Revenue Loss metrics in the

Potential Damage category and Investigation, Personnel, Customer Support, Repair and Recovery metrics in the Ex-Post Response Cost category. MAHP includes in Multiple Criteria Decision Algorithm (MCDA).

In order to develop risk estimation model, Tianshui et al. involved three elements, namely assets, vulnerability and threat [6]. Elements above were processed using three methods, namely: Decision Making Trial and Evaluation Laboratory (DEMATEL) to identify elements and evaluate the relationship between elements, Analytic Network Process (ANP) to give the distribution ratio to elements and Gray System Theory to generate risk level.

Alpcan et al. also conducted risk model development using linkages of business units (Nb), security threats (Nt) and people (Np) [7]. Risk Rank method was used to determine ranking and risk priority of security threat. Aplcan et al. stated that people (Np) can make mistakes in implementation of information technology. That mistakes can cause error and security threat (Nt) where it has impact to business unit (Nb) of enterprise. In order to estimate risk of security threat, enterprises must have capability to define the total value of inter-dependencies (Dpb) between Np and Nb. If the value of inter-dependencies between Np and Nb is represented by Єpb, then process of risk estimation can be illustrated in equation 1.

$$D_{pb} = \{N_p, N_b, Є_{pb}\} \qquad (1)$$

Studies above have involved business approach such as cost, business assets and business units. However, business approaches have not involved business characteristics from enterprises explicitly. As an illustration, an attack of security threat in large and small enterprises have different risk values. Large enterprise may have greater impact than small enterprises. It was stated by result of survey from Kaspersky Lab and B2B International that large enterprise has financial impact from IT securty incident about US$ 649.000 per year and SME (Small and Medium Enterprise) only has financial impact about US$ 50.000 per year [8].

Therefore, this paper tries to use different perspectives related metrics of business characteristics to develop risk model. In our previous work, we have validated five metrics to measure risk of security threat so this paper uses that metrics. Metrics used in this paper are organization size, organizational type, critical level, reputation and financial impact [9].

III. METHOD

This paper uses a quantitative approach to estimate the risk of security threat because quantitative approach is considered more reliable [10]. In order to generate weight of metrics, this paper uses Analytic Hierarchy Process (AHP) method which refers to Multi Criteria Decision Making (MCDM) algorithm. MCDM is generally used by decision makers for making alternative rankings. The alternative in MCDM can be defined as choice of solution in a problem [11].

One type of MCDM is a compensatory type where it has capability to evaluate several criteria and support trade-off system between attributes [12]. Analytic Hierarchy Process (AHP) is one of MCDM methods where it implements compensatory characteristic [12]. AHP can apply to qualitative and quantitative attributes [13] and it uses a linear structure (hierarchy) for making decisions [14]. In this paper, AHP is used as a weighting method for making decision from metrics namely critical level (CL), financial impact (FI), reputation (RE), organization size (OS) and business type (BT) [9]. Steps of measuring risk with AHP method is explained below.

A. Building of Hierarchy

Hierarchical structure of AHP is built using metrics of risk model as attribute of AHP. Output of AHP is risk value of information security threat. Therefore, hierarchical structure in this paper will be shown in Figure 1.

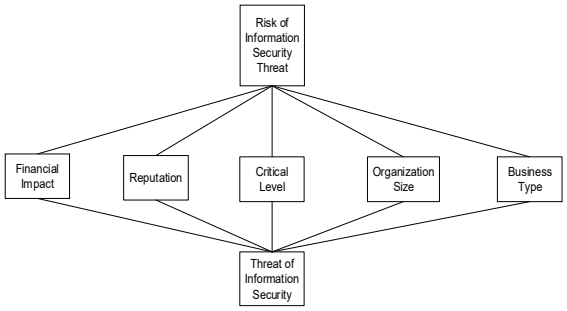

Figure 1: Hierarchy of AHP for measuring risk

B. Forming of Pairwise Comparison Matrix

Pairwise comparison matrix is formed by following hierarchy structure. The pattern of matrix can be shown Figure 2.

	FI	RE	CL	OS	BT
FI	1	a	b	c	d
RE	1/a	1	e	f	g
CL	1/b	1/e	1	h	i
OS	1/c	1/f	1/h	1	j
BT	1/d	1/g	1/i	1/j	1

Figure 2: Matrix of pairwise comparison

C. Calculation of normalized eigen

If *n x n* (*M*) matrix condition is multiplied by a non-zero column vector (*v*), it will produce value that equal with value of multiplication from scalar coefficient (λ) with nonzero column vector (*v*). The condition can be represented in equation 2.

$$M.v = \lambda.v \qquad (2)$$

So it can be concluded that the scalar coefficient is characteristic value from M variable. The scalar coefficient in this condition is often called eigen coefficient (λ) and the non-zero column vector is often called the eigen vectors (v). In this study, the eigen vectors (v) represents weight of each metrics.
Based on equation 2 above, eigen coefficient can be generated by following steps (equation 3 and 4).

$$(M - \lambda)v = 0 \qquad (3)$$
$$(M - \lambda) = 0 \qquad (4)$$

In order to perform reduction operation to the matrix, the scalar coefficient (λ) must be multiplied by the identity matrix (*I*) to produce matrix in same order (equation 5 and 6).

$$(M - \lambda.I) = 0 \qquad (5)$$
$$\det|M - \lambda.I| = 0 \qquad (6)$$

Eigen coefficient is produced by calculation from equation 6 and eigen vectors are produced by calculation from equation 2.

D. Consistency testing

Consistency testing for judgements of attributes is conducted using coefficient of consistency ratio (*CR*). The judgements of attributes are consistent if coefficient of consistency ratio is equal or less than 0.1 [15]. Consistency ratio can be computed using equation 7.

$$CR = \frac{consistency\ index}{random\ consistency\ index} \qquad (7)$$

However, consistency ratio can be defined if consistency index (CI) and random consistency index have been calculated. In order to compute consistency index, eigen vectors from previous step are involved to generate λ_{max}. Consistency index can be computed with equation 8.

$$CI = \frac{\lambda_{max} - n}{n - 1} \qquad (8)$$

In order to generate random consistency index, number of attributes or metrics (*n*) in matrix must be mapped in table of random consistency index. Table of random consistency index is shown in Table 1 [16], [17].

Table 1
Table of random consistency index

n	Random consistency index
1	0
2	0
3	0.58
4	0.9
5	1.12
6	1.24
7	1.32

E. Estimating Risk

Weight of metrics (*w*) is represented by eigen vectors. Weight of threat (*M*) can measured by number of exposed sensitive information. If value of risk is represented by variable *R*, then calculation of risk value can be conducted using equation 9.

$$R = \sum_{i=1}^{n} M_i \, x \, w_i \qquad (9)$$

n is number of metrics. In this paper, number of metrics is five, i.e. organization size, reputation, business type, critical level and financial impact.

IV. Experimental Details

This part needs two type of data. First data contains expert opinion related valuation of metrics. It is processed in AHP method to result weight of metrics. In order to gather first data, this paper uses questionnaire. All respondents in this study have work experience more than five years and they have education

background in information technology. They also have good understanding in information security field. It can describe that respondents have capability to understand questionnaire and problem in this study. Second data contains value of threat where it is gathered from two different enterprises.

AHP method processes data of metrics valuation. The output from AHP process is matrix of normalized eigen (Figure 3) and eigen vectors (Figure 4).

	FI	RE	CL	OS	BT
FI	0.48	0.627	0.466	0.302	0.235
RE	0.16	0.209	0.349	0.302	0.294
CL	0.12	0.070	0.116	0.302	0.176
OS	0.12	0.052	0.029	0.075	0.235
BT	0.12	0.042	0.039	0.019	0.059

Figure 3: Normalized eigen matrix

$$\begin{bmatrix} 0.422 \\ 0.263 \\ 0.157 \\ 0.102 \\ 0.056 \end{bmatrix}$$

Figure 4: Eigen vectors

In order to generate value of threat, this paper assesses data from disclosed information in two enterprises. Steps of gaining disclosed information in this experimental is show in Figure 5.

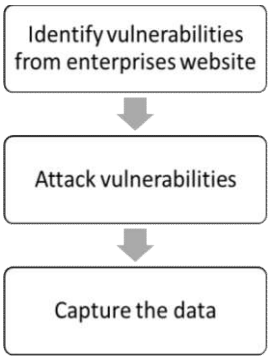

Figure 5: Steps of disclosed information gathering

V. Result and Discussion

Experimental process in previous part results two things, namely weight of metrics and value of threat. Eigen vectors are defined as weight of metrics where it is specifically shown in Table 2.

Table 2
Weight of metrics

Metrics	Weight
Financial Impact (FI)	42,2 %
Reputation (RE)	26,3 %
Critical Level (CL)	15,7 %
Organization Size (OS)	10.2 %
Business Type (BT)	5,6 %
Total	100 %

In order to compute value of threat, this paper uses classification method where it is based on sensitivity of information from disclosed data. The result is shown in Table 3.

Table 3
Value of threat from two enterprises

Metrics	FI	RE	CL	OS	BT
Enterprise 1	308.660	0	1	3	0
Enterprise 2	0	349.866	1	3	0

In Table 3, enterprise 1 has number of sensitive information about 308.660 records where it has financial impact to enterprises 1. Enterprise 2 has number of sensitive information about 349.866 records where it has effect to reputation of enterprise 2. Organization size is divided by three categories namely small (1), medium (2) and large (3) and both of enterprises are large enterprises. Both of enterprises also have information as critical asset for organization. It indicates that exposing information illegally may cause serious failure for all sectors in enterprise. Business type in this paper is categorized by two class namely financial organization (1) and non-financial organization (0). It is based on perspective that financial organization generally has higher potential in threat than non-financial organization [18]. In this paper, enterprise 1 has business type in hotel company and enterprise 2 has business type in health organization.

In order to measure weight of risk, this paper uses equation 9 above and the result can be shown in Table 4.

Table 4
Weight of risk in AHP method

Metrics	FI	RE	CL	OS	BT	Weight of Risk
Enterprise 1	130.25	0	0.157	0.306	0	130.72
Enterprise 2	0	92.01	0.157	0.306	0	92.48

In Table 4, risk estimation of information security threat can be performed and it results weight of risk. Enterprise 1 has higher risk than enterprise 2. It describes that enterprise 1 has higher priority than enterprise 2 in implementing of mitigation procedures.

This model is also possible to apply in an enterprise where it has several threats. It can be used to make mitigation priority between threats in an enterprise. Weight of risk in this model also accommodates business perspective where it has been represented by five metrics namely financial impact, critical level, reputation, organization size and business type.

VI. CONCLUSION

Risk estimation from information security threat is important process to map weight of risk to threat. The result of mapping is used to consider mitigation priority. High value of weight becomes high priority for enterprise to apply mitigation procedures quickly. However, in order to obtain proper weight of risk from information security threat, risk estimation must accommodate business approach so several business aspects is needed to be involved as metrics like financial impact, critical level, reputation, business type and organization size. In order to determine weight each business aspects, Analytic Hierarchy Process (AHP) is possible to be applied as method of priority calculation. Result from experimental states that combination between business aspects and Analytic Hierarchy Process (AHP) can be used to develop risk model where it can handle priority feature. The model can be implemented to measure risk priority between enterprises and it also possible to be implemented to measure risk priority between threats in an enterprise.

REFERENCES

[1] F. Sidi *et al.*, "Towards an Enhancement of Organizational Information Security through Threat Factor Profiling (TFP) Model," *J. Phys. Conf. Ser.*, vol. 892, no. 1, 2017.

[2] U. B and K. Kandasamy, "PROFILING THREAT MODELING APPROACHES AND METHODOLOGIES FOR IT AND CLOUD COMPUTING," *Int. J. Pure Appl. Math.*, vol. 115, no. 8, pp. 121–126, 2017.

[3] OWASP, "OWASP Risk Rating Methodology," 2015. [Online]. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[4] FIRST, "Common Vulnerability Scoring System v3.0: Specification Document," pp. 1–21, 2015.

[5] H. Ghani, J. Luna, and N. Suri, "Quantitative assessment of software vulnerabilities based on economic-driven security metrics," *2013 Int. Conf. Risks Secur. Internet Syst.*, pp. 1–8, 2013.

[6] W. Tianshui and Z. Gang, "A new security and privacy risk assessment model for information system considering influence relation of risk elements," *Proc. - 2014 9th Int. Conf. Broadband Wirel. Comput. Commun. Appl. BWCCA 2014*, pp. 233–238, 2015.

[7] T. Alpcan and N. Bambos, "Modeling dependencies in security risk management," *2009 Fourth Int. Conf. Risks Secur. Internet Syst. (CRiSIS 2009)*, pp. 113–116, 2009.

[8] Kaspersky Lab ZAO, "Global Corporate IT Security Risks : 2013," *Kaspersky*, no. May, 2013.

[9] P. D. Ibnugraha, L. E. Nugroho, and P. I. Santosa, "Metrics Analysis of Risk Profile : A Perspective on Business Aspects," in *International Conference on Information and Communications Technology (ICOIACT)*, 2018, pp. 275–279.

[10] S. Bakshi, "Performance Measurement Metrics for IT Governance," *ISACA J.*, vol. 6, pp. 21–27, 2016.

[11] Z. Qu, C. Wan, Z. Yang, and P. T. Lee, "Multi-Criteria Decision Making in Maritime Studies and Logistics," in *Multi-Criteria Decision Making in Maritime Studies and Logistics*, vol. 260, no. Mcdm, 2018, pp. 7–30.

[12] M. Majumder, "Impact of Urbanization on Water Shortage in Face of Climatic Aberrations," Springer-Verlag Singapur, 2015, pp. 35–48.

[13] A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security," *2014 IEEE 13th Int. Conf. Trust. Secur. Priv. Comput. Commun.*, pp. 284–291, 2014.

[14] A. Azizi and R. Maleki, "Comparative Study of AHP and ANP on Multi- Automotive Suppliers with Multi-Criteria," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, 2014, vol. II.

[15] N. A. A. Bakar, S. Harihodin, and N. Kama, "A priority based enterprise architecture implementation assessment model: An analytic hierarchy process (AHP) approach," *J. Telecommun. Electron. Comput. Eng.*, vol. 9, no. 2–3, pp. 121–125, 2017.

[16] T. D. Puspitasari, E. O. Sari, P. Destarianto, and H. Y. Riskiawan, "Decision Support System for Determining Scholarship Selection using an Analytical Hierarchy Process Decision Support System for Determining Scholarship Selection using an Analytical Hierarchy Process," in *The 2nd International Joint Conference on Science and Technology (IJCST)*, 2018.

[17] J. Franek and A. Kresta, "Judgment Scales and Consistency Measure in AHP," *Procedia Econ. Financ.*, vol. 12, no. March, pp. 164–173, 2014.

[18] A. Clark, T. T. Tan, C. Barbee, J. Donker, A. Palmer, and E. Skramstad, "Threats to the Financial Services Sector: Financial Services Sector Analysis of PwC's 2014 Global Economic Crime Survey," 2014.

eISBN 978-967-2348-14-6