*2014 International Symposium on Biometrics and Security Technologies (ISBAST)*

# Towards Metamodel-based Approach for Information Security Awareness Management

Ahmed Yousuf Jama, Maheyzah Md Siraj, Rashidah Kadir
Information Assurance and Security Research Group
Faculty of Computing
Universiti Teknologi Malaysia
81310 Skudai, Johor, Malaysia
axmed775@hotmail.com,{maheyzah, rashidah}@utm.my

***Abstract*—Information technology and information system have been used widely in many fields such as in business, education, marketing, transportation and medical. Security aspect plays a vital role and thus turns into a challenging issue. The security should be readily installed and resistance to various numbers of potential attacks likes Spyware, Phishing / Spam and Malwares (Virus, Worm and Trojans). It is important to have specific countermeasures that could minimize the harm to enterprises. Thus, increasing the awareness to optimal level is the main target of enterprise management. Unfortunately, the main reason that fails many existing enterprise' Information Security Awareness Management (ISAM) models is the complexity and inflexibility. Complexity means the model's structure is less practical (for instance, the implementation needs to be deployed manually). Inflexibility means it cannot support multiple kinds of businesses and did not consider security aspects. In this paper, we surveyed and discussed several existing ISAM models considering the security issues in current enterprise. We proposed a metamodel-based approach for ISAM that can offer efficiency and security that brings out clearly significant benefits by highlighting the organization overall level of awareness whether it is strong enough or weak. This will help many users in this domain to easily understand the important concepts required for their own information security awareness management.**

***Keywords—information security awareness, management evaluation, threat, malware, enterprise system*.**

## I. INTRODUCTION

Information security awareness management is one of the crucial aspects of securing information systems. Each enterprise in the world has many sensitive data and one of the challenges is how to preserve the confidentiality, integrity and availability of their data against attacks and threats [1]. Security Awareness (SA) is conducted to identify the safeguards to be adapted in every enterprise [2]. The enterprise has laboured to increase the number of account holders in an effort to raise their cash deposits. They have also leveraged on technology in an effort to increase revenues through alternative channels such as mobile and Internet banking. The increasing usage and reliance on information systems indicates that the banking enterprise are continuously collecting and storing information about their clients, as well as the enterprises' huge amount business intelligence information. Most enterprises have made heavy investments in information security technology, and continue to do so. One very fundamental aspect is an information security awareness management, which is not covered by technology and completely relies on lack of humans' or employee awareness on avoiding huge damage to the enterprise. In an effort to continuously improve their information security, enterprise has implemented information security awareness programs and campaigns to reduce the vulnerability inside and outside. Most of the enterprises face many challenges regarding the security breaches. For instance, the enterprise confidentiality, integrity and availability will be based on securing their system. Therefore, the thrust of enterprise policy will help the enterprise to increase confidentiality and privacy for its information [3]. Many attempts have been made to get an effective solution for dealing with different kind of security breaches. There are different kinds of methods in various aspects (mostly focuses on the technical prospective rather than management) have been proposed. Researchers have proven that information security commonly measured as a technological problem rather than a technological solution [4]. Intuitively, prevention is better than cure. Definitely, to maintain that security is more common sense. An enterprise should focus on a management subject rather than a technical one. Therefore, managing awareness is very crucial in information security since it can save costs and very practical. Assessing the linkage between the security and assets is the best way to protect the assets. In this paper, we focused on surveying existing studies and models on Information Security Awareness Management (ISAM). We also identify the weak areas that need to be addressed, for the last 20 years.

The rest of the paper is organized as follows. Section II highlights some related works in security awareness management models. Section III proposes the methodology for developing the ISAM Metamodel. Section IV discusses the validation techniques for proposed ISAM Metamodel. Section V presents the initial finding for ISAM Metamodel. Lastly, we conclude the paper and recommend some future works.

978-1-4799-6444-4/14/$31.00 ©2014 IEEE

## II. Related Work

In general, the main objective of Information Security Awareness (ISA) is to provide protection of enterprise assets, and other form of activities to ensure effective operational adherence in the system as defined and articulated by [1]. Information security is crucial for organizations. In today's technology, information security makes communication possible for the world with high quality, secure and comprehensive environment. Moreover, the correct information is central in supporting security awareness program the right way. Therefore, securing information resources for the organization is crucial to check that the procedures for organizing rather well protected from attacks, virus, worms, and social engineering that threaten to enterprises around the world. It is very important for enterprises to have information security awareness, and people training to their employees.

ISA provides rules and regulations in enterprises to construct, develop and maintain security of their computer supported hardware and software resources. The set of policies explaining the technique in which computer resources can be used and protected [4]. From the information security point of view, expert states that security does not mean only protect the computer system from malicious code like viruses. But, it can be applied in different areas and it means defending an enterprise most expensive asset from any attack faced whether inside or outside [7].

Kruger and Kearney [11] mentioned that ISA is a self-motivated and ongoing process prepared extra complex towards threats to constantly adapt to the current environment. They also proposed in [11], a method on testing ISA that makes use of cognitive psychology. Pointing the use of social psychology as one of the effective means to use for purposes of conducting effective awareness on information security among practitioners.

According to ENISA report released in 2007 [6], a study has been conducted on European enterprises that practice information security strategy and implementation. Eighteen items were identified as the main techniques used to impart awareness. The respondent enterprises were required to select which techniques used, and the results will be different strategies of different enterprises. Candidacy [5] proposed a causal assessment model with a powerful inference engine that analyses and quantifies information security awareness that are due to various threat sources on the enterprise. Meanwhile, Abdisalam and Munir [18] provides the essential concepts of any awareness management plan through threats that are evaluated and the vulnerability that is related to the system assets by looking at different case study as a factor of threats, vulnerability and impacts on information assets. While work by Xinrong [29] based his analysis on ISO27001 series standards to propose measures for information security awareness evaluation on the e-campus systems that involves assets, threats, and vulnerability.

Kondakci [15] also provides a cost model that could be used to analyze the impacts of Internet malware threats to enable cost estimates to be made based on the incidents caused and the lack of awareness incurred on the employee. The work shows that analysis of malware propagation on the network alone will not be realistic without relating it to the entire system performance, its economic losses and the overall risk incurred on the assets [15]. Lack of ISAM in enterprise workflow can cause many threats to the enterprise structure. For example, the number of attacks in 2010 is increasing (approximately 90 per day). This result also explains that 70% of attacks focused on big companies and 15% of the attacks mostly focused on small enterprise [28]. The result shows that the target enterprise in the world was dramatically increased suddenly. Such scenario has started since 2006 as shown in Figure 1.

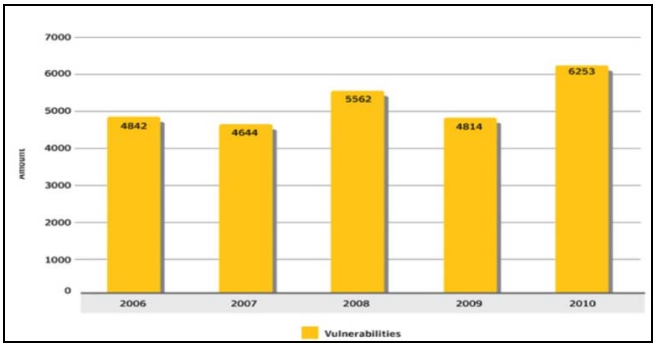


Fig. 1. Total number vulnerabilities identified in 2006-2010 [28]

Figure 1 explains the total vulnerabilities identified between 2006 until 2010 and this result show the amount of attack increase for the three years causing big damage for the enterprise around the world. Intuitively, this will increase the number of attacks as well.

In summary, many authors have proposed different types and levels of innovative models on measuring awareness for an enterprise. Each model has its own unique features and some of them are very simple but effective. The three main factors need to be measured are user behaviour, attitude and knowledge possessed in as far as Information Security is concerned. Risk-based assessments are used to decided which areas of the business to focus on as far as awareness is concerned [8].

Simplicity while attempting to cover as much ground as possible on items considered is important for respective enterprises. In conclusion, before a measurement model is defined and tested, the key considerations of the business must be identified, and must have adequate representation in the model [13].

### *A. Comparative Analysis*

Table I shows the existing proposed models on ISAM to minimize the threats faced by organization assets. Some models focused on aspects after the danger happens, while the others focused on preventing the damage (before the danger happens).

TABLE I. COMPARISON OF EXISTING MODELS BASED ON DETECTION AND PREVENTION OF THREATS

| Existing Model | Detection | Prevention |
|---|---|---|
| ISRA Model [14] | ✓ | ✓ |
| Kruger and Kearney model [13] | ✓ | ✓ |
| Candidacy model [5] | ✓ | ✓ |
| Abdisalam and Munir model [19] | ✓ | ✓ |
| Kajava and Savola Perspective [12] | ✓ | ✓ |
| Siponen model [21] | ✓ | × |
| ENISA model [6] | ✓ | × |
| Mozilla model [23] | ✓ | × |

### B. *Information Security Awareness Effectiveness*

The effectiveness of existing models are represented in the format of one (1) being the least effective until five (5) being the most effective progressing from bottom to top. Induction soon after employment was selected by the highest number (10) of respondents compared to the other models as the most effective model to spread information security awareness in an enterprise; or another model also selected as the most effective after induction is inclusion of security responsibilities in employment contracts based on the number (5) of respondents. The results indicate that in terms of effectiveness, all information security awareness models were considered as generally effective, (i.e. most of the respondents selected between 3 to 5 on the like scale indicating that in general, most respondents did not select 1 and 2 in the like scale which were representing their opinion in terms of least the effectiveness of their Information Security models). Other opinions offered by the respondents indicate that they considered Senior Executive management support and participation of information security awareness as a very effective approach of imparting information security awareness models. In terms of the use of a quiz as an information security evaluation, one of the respondents argues that scenario-based questions are better suited towards spreading information security awareness than direct knowledge-based questions.

## III. THE PROPOSED METAMODEL

The proposed ISAM Metamodel (ISAMM) is based on three stages as shown in Fig. 2. Firstly, in order to initiate and create a new metamodel, 10 existing related models are being studied and analysed. This is to identify the general, important and practical key concepts required by an enterprise for implementing effective and comprehensive information security awareness. In the second stage, we found that with the combination of the three related ISAM models ([17] is very relevant and comply with the current requirements of information security awareness. Based from these works, a new metamodel for ISAM is designed and proposed. The detail on the architecture design of the proposed metamodel can be found in Section V. There are three types of validation need to be conducted to measure the effectiveness of the proposed ISAMM: frequency-based, face validity and tracing. With the responses from all validations, the design of ISAMM is being improvised.

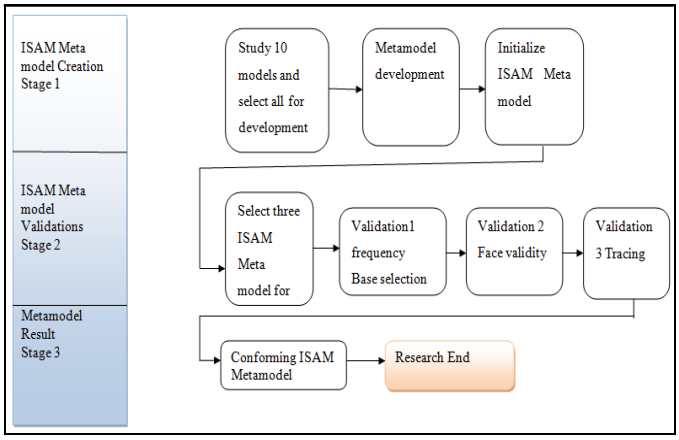


Fig. 2. The process involved in developing the proposed metomodel.

Apart from gathering and analyzing the key concepts for an ISAM that based on existing models, a set of questionnaires is also a useful tool to recognize the latest information security requirements and concepts for an enterprise. A questionnaire approach can be implemented by designing a survey that will explore the necessary key requirements of a model [14]. The model will then be validated through the analysis from the questionnaires. In addition, the use of questionnaires is justified to provide an effective and efficient way of gathering information within a very short time. Further, questionnaires facilitate easier coding and analysis of data collected. The questionnaires to be administered included a few open-ended questions. Because open-ended questions provide an insight of new ideas, whereas closed ended questions ensure that the respondents are restricted to certain categories of their responses, and it was designed to discover what factors influence user behaviour toward information security and impact of information security management [27].

Depending on the nature of the problem, a decision to use the questionnaires approach is based on the following reasons: Firstly, the use of a questionnaires approach allows a good fit to develop a correlation between the social reality of the research participants and the theory. Secondly, it enables the study of the cause of employee behaviour and the effect of different factors'

relationships. Thirdly, it will allow the study to assemble the common factors and then start to compare them to the action being taken in terms of security with the help of an in-depth analysis of the different types of data, raw data that can be converted into the meaningful results of the proposed work [16]. In addition, for analyzing the data in the most effective manner can use a number of different tools and techniques. In this context, it's necessary to conduct different statistical methods, including SPSS (Statistical Package for the Social Sciences) and different types of statistical tests.

## IV. Analysis On Survey For Metamodel Preparation

The collected data from the questionnaire was edited, and analyzed using SPSS. Data analysis was conducted in the format of descriptive statistics. Descriptive analysis can be described as a process that involves transforming a mass of raw data into tables, charts, with frequency distribution and percentages, which are a vital part of making sense of the data. The respondents' were gender, position in the organization, age, educational level, work experience in the enterprise. The statistics have shown that the respondents of male gender were 80%, while female 20%. This is an indicator of the fact that the information security industry is dominated by the male gender.

An analysis of the survey participants' responses revealed that 30% of the participants are employed in the 'Company' sector, 40% are working in the 'Academic' area and the remaining 30% is from 'Non-academic'. A total of 420 participants in the survey are considered for the analysis (because of their complete responses, and they are selected from the three sectors). The results show that the majority of the respondents (45%) are BSc graduates, about 35% respondents have an MSc, and 10% respondents are PhD degree holders and 10% respondents are educated to GCSE level. The majority of respondents (40%) are from the age group of 35-54 years, while 42% of the respondents belong to the age group of 25-34 years. About 8% of the respondents are from the age group of 19-24 years and remaining 10% of respondents are from the age group of over 55 years [25].

Table II shows the responses from the questionnaire in terms of usage frequency on information security items. The findings show that Information Security Policy with 95%, Information Security Guides with 90%, Information Security Staff manuals with 80%, Information Security Induction for New Employees with 70% and Information Security and responsibilities in contracts with 65% were the most frequently used Information Security Awareness techniques in most of their enterprises. The results also shown that the Information Security Awareness techniques, which had the lowest usage among the respondents, were information security posters with 25%, information security awareness content for different group targets by 30% and Quizzes on security matters with incentives with 20%. It had been identified that most enterprises do not have different content targeting different members of the enterprise (e.g. senior management content as compared to that of junior staff content). However, the existence of the different content would then make it more complex to measure enterprise information security awareness. The results presented two techniques that are used by half the number of respondents namely Information Security Messages in existing business courses with 50% and Computer based Information Security awareness with 50%. This means their position in terms of usage is mainly due to the gaining acceptance of the importance of information security awareness, hence their inclusion in the normal mainstream training courses that existed prior to the introduction of information security awareness courses [20].

TABLE II. The Frequency Of Usage In Information Security Items

| Variable | Frequency% |
|---|---|
| Information security policy | 95% |
| Internet information guides | 90% |
| Information security staff | 80% |
| Information security induction for new employee | 70% |
| Information security responsibilities | 65% |
| Information security leaflets | 60% |
| Information security posters | 25% |
| Information security emails | 85% |
| Information security awareness contents | 30% |
| Information security items like screen savers. | 45% |
| Information security messages | 50% |
| Computer based information awareness | 50% |
| Computer based security awareness | 40% |
| Class room based information security awareness | 55% |
| Class room information security awareness | 35% |
| Quizzes on security matters | 20% |

## V. Initial Results On Metamodel Design

This section presents the initial design of the proposed ISAM Metamodel. The metamodel has four phases that clarify the classes of awareness concepts and their relationships. The four phases are Awareness planning, Awareness assessment and evaluation, Awareness for threat mitigation and Awareness monitoring and review.

Fig. 3 assists the security experts to get feedback from organization in order to conduct their security awareness inside the organization, by assessing their attitude, behavior and knowledge for information security.

Fig. 4 assists the security experts to determine the likelihood of occurrence, the resulting consequence, and additional controls that would mitigate this impact. It also defines as part of awareness management process. This figure also mentions awareness, evaluation, which deeply explains the process of determining the significance of the awareness by comparing the result of the awareness analysis against giving awareness criteria.

Fig. 5 assists the security experts more specific for threat mitigation for selecting and implementing the best security response action that are recommended in Phase 2 (Fig. 4) in order to minimize the threats based on the priority. These controls help to mitigate the threats faced by information security.

Fig. 6 explains threats, vulnerabilities likelihood may change abnormally without any indication, and therefore constant monitoring is important to detect these changes. This phase also deeply explains ongoing assessment of awareness in order to ensure effective response action to control the threats faced by organizations.

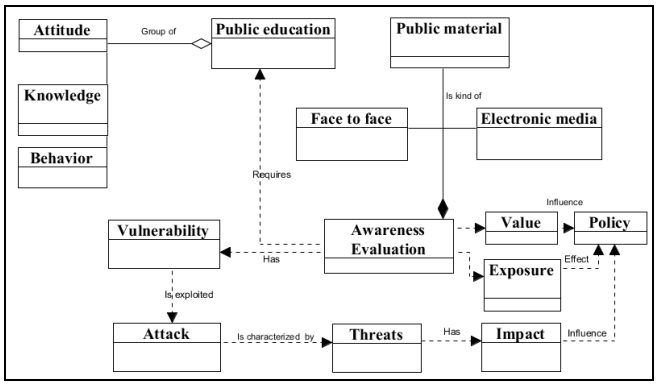


Fig. 3. Phase 1: Awareness planning

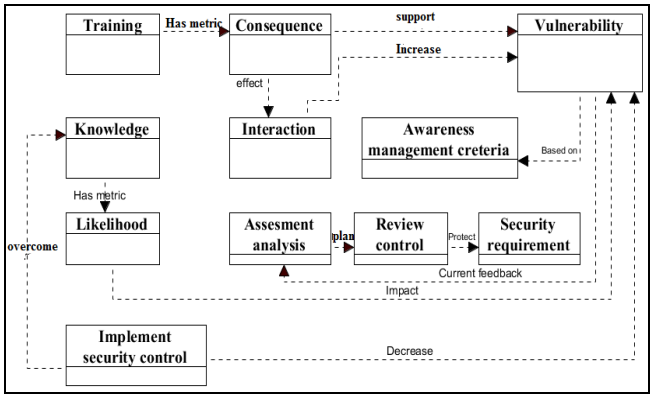


Fig. 4. Phase 2: Awareness assessments and evaluation

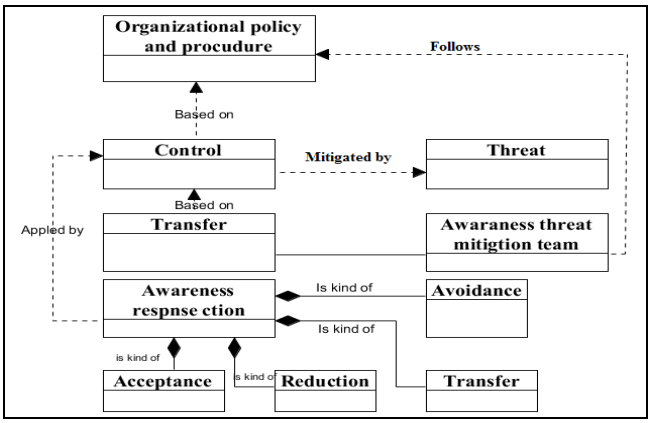


Fig. 5. Phase 3: Awareness for threat mitigation

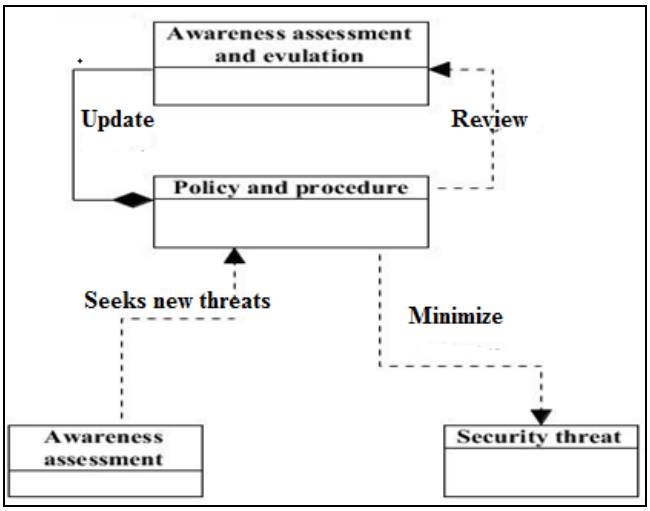


Fig. 6. Phase 4: Awareness monitoring and review

## VI. CONCLUSION

The results presented in this paper can be categorized into were two parts. The first part was looking at the various techniques used to impart awareness and their effectiveness. The second part was served on various models used to measure awareness levels in the enterprise and seeking the input of the industry professionals. Their input will be important in the design of the awareness measurement models for the research. Analysis of the awareness questionnaire indicated that most enterprises are already conducting awareness initiatives at various levels and capacities. It also showed that most of the same enterprises are facing challenges in terms of both carrying out awareness activities and measuring awareness levels. Following the analysis of the responses received, the results indicate that a model to measure awareness levels in enterprises is necessary since there is a need to measure awareness levels. The proposed metamodel will also incorporate the input from the analysis in order to make it more feasible and practical to

implement in any enterprises. Based on the questionnaire analysis, it has been found that employees in the academic area better at following and implementing information security policies as compared to other sectors. The reason for this is that academic sector employees have better awareness, and good communication and reward systems. Moreover, employees in the health sector have a positive attitude towards preventing damage rather than dealing with it.

## ACKNOWLEDGMENT

We would like to thank Ministry of Higher Education (MoHE) and Universiti Teknologi Malaysia for funding this work under Potential Academic Staff research grant with reference number PY/2014/02899.

## REFERENCES

[1] Bertino, E., Khan, L. R., Sandhu, R. and Thuraisingham, B. (2006). "Secure knowledge management: confidentiality, trust, and privacy". Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on. 36(3), pp. 429-438.

[2] Colwill, C. (2010). "Human factors in information security: The insider threat: Who can you trust these days?", Science direct-information security technical report.

[3] Costa, P. D., Almeida, J. P. A., Pires, L. F., gizzard, G., and van Sinderen, M. (2006). "Towards conceptual foundations for context-aware applications". Proceedings of the Third International Workshop on Modelling and Retrieval of Context (MRC06), Boston, USA.

[4] Chiprianov, V., Kermarrec, Y., Rouvrais, S., and Simonin, J. (2012). "Extending enterprise architecture modelling languages for domain specificity and collaboration: application to telecommunication service design". Software & Systems Modelling, pp. 1-12.

[5] Dagger, D., Conlan, O., and Candidacy, V. (2009). "Architecture for candidacy in adaptive modeling systems to facilitate the reuse of learning Resources". In World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, pp. 49-56.

[6] European Network and Information Security Agency (ENISA). Information Security Awareness Initiatives: Current Practice and the measurement of success. 2007.

[7] Fafchamps, D. (1994). "Organizational factors and reuse". Software, IEEE. 11(5), pp. 31-41.

[8] Fenz, S. and Ekelhart, A. (2011). "Verification, Validation,and Evaluation in Information Security Risk Management". In Fenz, S. & Ekelhart, A. (Eds.), Information Security Risk Management.

[9] Happel, H.-J. and Seedorf, S. (2006). "Applications of ontologies in software engineering". Proceedings of the 2006 Proc. of Workshop on Sematic Web Enabled Software Engineering (SWESE) on the ISWC: Citeseer, pp. 5-9.

[10] Issa-Salwe, A. M. And Ahmed, M. (2011). "Management of an Information System by Assessing Threat, Vulnerability and Countermeasure".

[11] Kruger, H., and Kearney, W. (2006). "A prototype for assessing information security awareness". Computers & security, 25 (4), pp. 289-296.

[12] Kajava, J., and Savola, R. (2007). "Towards better information security management by understanding security metrics and measuring processes". Proceedings of the European University Information Systems (EUNIS).

[13] Kruger, H. and Kearney, W. (2008). "Consensus ranking–An ICT security awareness case study". Computers & security. 27(7), pp. 254-259.

[14] Kritzinger, E. and Smith, E. (2008). "Information security management: An information security retrieval and awareness model for industry". Computers & security. 27(5), pp. 224-231.

[15] Kondakci, S. (2010). "Network Security Risk Assessment Using Bayesian Belief Networks". IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust.

[16] Kim, I.-G., Bae, D.-H. and Hong, J.-E. (2007). "A component composition model, providing dynamic, flexible, and hierarchical composition of components for supporting software evolution". Journal of Systems and Software. 80(11), pp. 1797-1816.

[17] Othman and Beydoum. Metamodel Development Steps performance, 2009.

[18] Munir, M and Abdisalam. (2010). "Simplified model of awareness process in a information awareness management for real-time operation". International Journal of Vehicle Systems Modeling and Testing, 5(4), pp. 347-357.

[19] Puhakainen, P. and Siponen, M. (2010). "Improving employees' compliance through information systems security training: an action research study". Mis Quarterly. 34(4), pp. 757-778.

[20] Susanto, H. and Almunawar, M. (2012). "Information Security Awareness Within Business enviroment".

[21] Siponen, M. T. (2000). "A conceptual foundation for organizational information security awareness". Information Management and Computer Security, 8(1), pp. 31-41.

[22] Viduto, V., Maple, C. and Huang, W. (2010). "An analytical evaluation of network security modelling techniques applied to manage threats", IEEE 2010 International Conference on Broadband, Wireless Computing, Communication and Applications.

[23] Valiente, M.-C., Vicente-Chicote, C. and Rodríguez, D. (2011). "An Ontology-Based and Model-Driven Approach for Designing IT Service Management Systems". International Journal of Service Science, Management, Engineering, and Technology IJSSMET , 2 (2) , pp. 65-81.

[24] Van Niekerk, J. and Von Solms, R. (2004). "Organisational learning models for information security". Proceedings of the 2004 The ISSA 2004 Enabling Tomorrow Conference.

[25] Waly, N., Tassabehji, R. and Kamala, M. (2012). "Improving Organisational Information Security Management: The Impact of Training and Awareness". Proceedings of the 2012 High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), pp. 1270-1275.

[26] Wee Beng, G., Lee, K. and Loh, R. (1994). "Towards a more realistic appraisalof, IT impacts and outcomes a case study analysis based on the structurational model of information technology". Proceedings of the IEEE Region 10's Ninth Annual International Conference, 131, pp. 133-138.

[27] Yan, X. and Linn, C. (2010). "Terms Frequency Based Feature Selection Methods for Text Categoriztion". Proceedings of the Fourth International Conference on Generic and Evalutionary Computing (ICGEC 2010), pp. 280-283.

[28] Zhang, Z., Wang, S., and Kadobayashi, Y. (2012). "Exploring attack graph for cost-benefit security hardening: A probabilistic approach". Computers & security.