Information Security Risk Assessment by using Data Mining – A Review

K.Madhavan
Research scholar Research & DevelopmentCentre Bharathiar University Coimbatore - 641 046, Tamilnadu.

Dr.R.ManickaChezian
Associate Professor Dept.of ComputerScience(Aided) NGM College (Autonomous) Pollachi-642 001, Tamilnadu.

Abstract – This paper reviews the recent works carried out by researchers in the field of information security risk assessment in organizations. Information security risk assessment empowers organizations to determine what threats exist to a specific asset and the associated risk level of that threat. The threat prioritization process provides the necessary information to the organizations to select appropriate control measures and initiate safeguarding and counter measures to minimize the risk to an acceptable level. The main purpose of the paper is to compare the previous work on information security risk assessment process advocated by different authors to identify the procedure adopted, method of the study, variables used and the major focus of the studies.

Index Terms – Information security risk assessment, risk assessment methods, quantitative risk assessment method, qualitative risk assessment method.

1. INTRODUCTION

Securing the information assets is considered as one of the greatest challenge to the organizations around the world. The cost involved in providing security to the information assets is increasing. Moreover, new threats and vulnerabilities to the systems are increasingly evidenced in the recent times. In order to develop framework solution to provide an effective information security risk assessment system to the organizations, it is important to study the existing system in detail. This paper attempts to review the published journals on information security risk assessment and management.

2. RELATED WORK

Karabacak and Sogukpinar (2005) have proposed quantitative approach named as Information Security Risk Analysis Method (ISRAM) to analyze the security risks of information technology assets. A survey was conducted with the managers and staff members. The results of statistical analysis of the survey data was used for simulating the risk environment and the risk model was created using Arena Simulation software. The major advantage of the approach over other risk analysis methods includes its ease of use, no complicated mathematical and statistical instruments. The results of the case study show that ISRAM has yielded consistent results in a reasonable time period. The authors suggested that ISRAM can be used for a wide range of problems.

Sahinoglu (2008) proposed a probabilistic measure to quantitatively estimate Software Security Risks. The proposed method named as security meter (SM) model was actually used to mimic the events of the breach of security. An empirical study was presented and verified by discrete-event and Monte Carlo simulations. The design was shown to improve as more data are collected and updated. Practical aspects of the SM were presented with a real world example and a risk-management scenario.

Sheung et al. (2009) have proposed a quantitative model for assessing cyber security risk in information security. The model could be used to evaluate the security readiness of firms in the marketplace through qualitative and quantitative tools. A Bayesian network methodology was proposed that can be used to generate a cyber-security risk score that takes as input a firm’s security profile and data breach statistics. The quantitative model enables cyber risk to be captured in a precise and comparable fashion. The objective of the scoring model was to create a common reference in the marketplace that could enhance incentives for firms to invest and improve their security systems. The work can be extended further by implementing the cyber risk-scoring model in the marketplace. The major drawback of the model is that a large sample size of participants is required to produce a statistically significant result to justify the use of this scoring model. An alternative technique would be to conduct a simulation to predict how the model would function given different scenarios.

Yang et al. (2009) have identified several limitations in the multi criteria methods that were more commonly used in the information security risk assessment systems. They found that most of these multi-criteria methods focus on the ranking and selecting information security risks. These methods were usually used to compare all alternatives based on the synthesized scorings within a normalized scale with respect to the same criteria in multi-criteria problems. However, the decision makers often simultaneously manage one or several alternatives/projects with conflicting and non-commensurable criteria to reduce the gaps to achieve the aspired grade in practice. They then need to rank the gaps that have not been reduced or improved (the unimproved gaps) for the alternatives/projects or aspects of a project to get the most benefit. Because these compared alternatives/projects do not usually have the same criteria/aspects, traditional methods are unsuitable to deal with them. Thus, this research proposes a new VIKOR method to solve this problem. The new method allows the decision maker to understand the gaps of the projects aspects and rank them to improve these large gaps in control items to achieve the aspired level.

Samy et al. (2010) have proposed a new method for risk analysis by effectively utilizing the existing risk management process framework which is more commonly used in medical domain namely survival analysis approach. The study used Cox Proportional Hazards (PH) Model to identify potential threats to information security. The risk management process was based on Australian/New Zealand Standard for Risk Management (AS/NZS 4360:1999). The integration of risk management process and survival analysis has added new insights and can lead to further research in major fields such as prognostic and health management, network reliability and survivability, software reliability and test measurements which is not fully explored yet using the proposed method.

Saripalli and Walters (2010) have proposed a quantitative risk and impact assessment framework (QUIRC) to assess the security risks associated with cloud computing platforms. This framework, called QUIRC, defines risk as a combination of the Probability of a security threat event and it’s Severity, measured as its Impact. Six keys Security Objectives (SO) were identified for cloud platforms, and that most of the typical attack vectors and events mapped to one of these six categories. Wide-band Delphi method was proposed as a scientific means to collect the information necessary for assessing security risks. Risk assessment knowledge bases could be developed specific to each industry vertical, which then serve as inputs for security risk assessment of cloud computing platforms. QUIRC’s key advantage is its fully quantitative and iterative convergence approach, which enables stakeholders to comparatively assess the relative robustness of different cloud vendor offerings and approaches in a defensible manner.

Amancei (2011) proposed a quantitative method for information security risk management. The study used questionnaire to assess the internal control, and through evaluation based on existing controls as part of vulnerability assessment. The method presented contains all the key elements that concur in risk management, as well as list of threats, resource classification and evaluation, correlation between risks and controls and residual risk computation.

Zambon et al (2011) have proposed qualitative method for risk assessment called as time dependency (QualTD) model and technique. The QualTD model was based on the quantitative time dependency (TD) model proposed by Zambon et al. (2007). The QualTD model was analyzed for 12 RA standard methods and can be employed together with standard risk assessment methods for the qualitative assessment of availability risks based on the propagation of availability incidents in IT architecture. The model can be embedded with the existing risk assessment methods in organization without taking too much time or unavailable information. The model was validated by conducting real time risk assessment on the authentication and authorization system of a large multinational company. The evaluation of results indicates that QualTD produced better results in terms of accuracy in estimation of impacts. QualkiTD was applicable to risk assessment to cases in which all the required information are unavailable. In addition, the model was effective in reducing the number of subjective decisions in risk assessment procedure. QualTD is more suitable in the assessment of availability of risks in IT infrastructures.

Winkelvos et al. (2011) believed that as the systems’ complexity grows, it becomes less feasible to calculate the probability of all patterns of a system’s behavior. Thus, a model based simulation of the system is advantageous in combination with a focus on precisely defined security properties. The paper proposed a property based approach to risk assessment aimed at assessing risks in a process-oriented or service level view of a system and also to derive a more detailed estimation on a technical level. A simulation tool named as Simple Homomorphism Verification Tool (SHVT)was developed based on the existing formal validation and verification. The tool has GUI for monitoring automation which facilitates the explicit definition of security properties to be investigated during the simulation cycles. The tool facilitated probabilistic simulation, providing information about the probability distribution of satisfaction or violation of specified properties. The advantage of the proposed method compared to other method lies in its approach of using relative weighting of classes of transitions which is less complex in terms of quality and quantity.

Shukla and Kumar (2012) have described some of the methodologies used currently to analyze information security risks. The main task for an organization is to determine which one to use. Since the organization spend money on whichever method they choose, it is vital that the chosen methodology meet the requirements. The purpose of the study is to compare and clarify the different activities, inputs, and outputs required by each model of information security risk assessment and the analysis that effectively addresses the risks of information security. At the moment, copious methodologies exist and many organizations are confronted with the frightening task of choosing one. The framework was developed with the aim of analyzing six methodologies in detail and recognizing some common criteria.

Burtescu (2012) used the Monte-Carlo method in order to model a set of security parameters that are used in security risk analysis. The frequency of unwanted events, damages and their impact was the main focus and both the quantitative and qualitative security risk analysis approach were used. The obtained results of the study serve as a guide for experts to better allocation of resources for decreasing or eliminating the risk and will also represent a warning for the leadership about certain absolutely necessary investments. Monte-Carlo simulation allow the risk analysis team to run different scenarios in order to be able to make estimations of all the possible future situations.

Tamjidyamcholo and Al-Dabbagh (2012) have proposed a genetic algorithm (GA) for reducing the Information Security risks in uncertain environments. The effectiveness of the proposed method was verified through an example.

Behnia et al. (2012) have proposed a methodology for information security risk analysis in which the assets, vulnerabilities, threats, and controls of an organization are linked. The main purpose of the study was to compare and clarify the different activities, inputs and outputs required by each model of information security risk assessment and the analysis that effectively addresses the risks of information security. The study aimed to develop a comfortable and reliable framework that organizations can apply to compare different information security risk analysis methodologies. The framework was developed with the aim of analyzing five methodologies in detail and recognizing some common criteria. The normal criteria have then been used to form the characteristics of the framework.

García and Fernández (2013) have analyzed most common methodologies used to assess the information security risks supported by computer systems. The results of the analysis show that most of methodologies are too simple and do not consider interrelations between assets explicitly. However, these interrelations always exist in the real computer systems. The Magerit methodology was illustrated in detail which represents the interrelations using graphs and provides support for a simple but effective qualitative and quantitative risk analysis considering the interrelations. This study shows that the Magerit methodology has a great capability to represent complex computer systems and it is very easy to use.

Kiran et al. (2013) have made a comparative study to equate the choice of methods that allow an organization to weigh their information security risk. They analyzed activities, inputs and outputs required by various information security risk assessment models and also analyzed which ones address information security risk effectively. The resulting information helps evaluating the models' applicability to an organization and their specific needs. It organize to authenticate and legalize the conclusions taken from the theoretical study of all these models and hence, reduce risk.

Ahmad et al. (2013) have presented a quantitative equation to assess the information security level for enterprises, establishments and corporate in general, and financial institutions in particular in public and private sectors in Syria. This method is the result of statistical study which has been applied to a set of financial institutions in Syria as a sample of study to assess the gap between existing information security level and ISO 27K directives for Information and Communication Technology (ICT) security, benefiting from other international approaches and models designed for this purpose. This study aims to highlight the special requirements and the modified framework required to develop ICT security in financial institutions taking into consideration the culture and the special conditions in Syria.

Hassan (2013) studied the impact of information security management on the effectiveness of applying e-management in the Governmental Organizations in Gaza. The research used the analytical descriptive approach and used comprehensive survey to collect the data from the respondents. Ten fields of information security management were investigated at eight Governmental Organizations along with the effectiveness of applying e-management. The ten fields of information security management include: Security Policy, Organizational Security, Assets Classification and Control, Personnel Security, Physical and Environmental Security, Computer and Network Management, System Access Control, System Development and Maintenance, Business Continuity Planning, Compliance to Legal Requirements.

Bojanc and Jerman-Blažič (2013) have presented a mathematical model for the optimal security-technology investment evaluation and decision-making processes based on the quantitative analysis of security risks and digital asset assessments in an enterprise. The model makes use of the quantitative analysis of different security measures that counteract individual risks by identifying the information system processes in an enterprise and the potential threats. The selection of security technology is based on the efficiency of selected security measures. Economic metrics are applied for the efficiency assessment and comparative analysis of different protection technologies. Unlike the existing models for evaluation of the security investment, the proposed model allows direct comparison and quantitative assessment of different security measures.

Lee and Chang (2014) employed a combination of fuzzy method and decision tree (DT) to evaluate the information security risk assessment for decision-makers. The study was aimed to apply fuzzy method to improve the testing accuracy for the DT. The proposed method was tested in the attendance management system of a government agency. The study identified 155 input-output data with 22 attributes for measuring the value at risk obtained from ISO/IEC 27001 information security management system (ISMS) standard and ISO/IEC 27005: 2008. The accuracy of the proposed system was compared other approaches like decision tree, FCM, BPN and SVM techniques. The results show that the proposed method outperformed other methods. In addition, zoo dataset collected from UCI repository was also used to test the performance of the proposed algorithm. From simulation results, the proposed approach outperforms other existing approaches.

Ghazouani et al. (2014) have proposed a method for mathematical formulation of risk by using the lower level granular elements of risk like threat, probability, criteria used to determine an asset‘s value, exposure, frequency and existing protection measure. The proposed method was based on ISO 27005 and integrates risk management models like Mehari, EBIOS, CRAMM and SP800-30(NIST). The study used quantitative method and using mathematical formulation, the risk score was derived. The study was a part of a larger project to develop an actual web-based Information Security Risk Management Tool.

3. CONCLUSION

This paper provided a detailed review of recent studies on information security risk assessment. Current practices in information security risk assessments analyzed in detail by reviewing various studies carried by other researchers in this area. Based on the extensive review, following observations were made:

- Most of the studies on risk assessment are using quantitative approach in which the questionnaire based surveys are being conducted with key stakeholders and results are analyzed.
- Several studies have attempted simulation software based approach to model the perceived threats to the existing information assets (Karabacak&Sogukpinar, 2005; Sahinoglu, 2008; Winkelvos et al., 2011; Burtescu, 2012)..
- Soft computing methods like rough sets, grey sets, fuzzy systems, genetic algorithm, support vector machine, and Bayesian network and hybrid model are increasingly used in risk assessment.
- Few studies have also attempted hybrid models in which two or more existing models are integrated to develop the new model.

REFERENCES

[1] Shukla, N., & Kumar, S. (2012). A comparative study on information security risk analysis practices “on Issues and Challenges in Networking. *Intelligence and Computing Technologies–ICNICT*.

[2] Karabacak, B., &Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), 147-159.

[3] Sahinoglu, M. (2008). An Input–Output Measurable Design for the Security Meter Model to Quantify and Manage Software Security Risk. *Instrumentation and Measurement, IEEE Transactions on*, *57*(6), 1251-1260.

[4] Samy, G. N., Ahmad, R., & Ismail, Z. (2010, August). A framework for integrated risk management process using survival analysis approach in information security. In *Information Assurance and Security (IAS), 2010 Sixth International Conference on* (pp. 185-190). IEEE.

[5] Saripalli, P., & Walters, B. (2010, July). Quirc: A quantitative impact and risk assessment framework for cloud security. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 280-288). IEEE.

[6] Zambon, E., Etalle, S., Wieringa, R. J., &Hartel, P. (2011). Model-based qualitative risk assessment for availability of IT infrastructures. *Software & Systems Modeling*, *10*(4), 553-580.

[7] Winkelvos, T., Rudolph, C., &Repp, J. (2011, August). A property based security risk analysis through weighted simulation. In *Information Security South Africa (ISSA), 2011* (pp. 1-8). IEEE.

[8] Samy, G. N., Ahmad, R., & Ismail, Z. (2012). *Adopting and Adapting Medical Approach in Risk Management Process for Analysing Information Security Risk*. INTECH Open Access Publisher.

[9] Samy, G. N., Ahmad, R., & Ismail, Z. (2010, August). A framework for integrated risk management process using survival analysis approach in information security. In *Information Assurance and Security (IAS), 2010 Sixth International Conference on* (pp. 185-190). IEEE.

[10] Burtescu, E. (2012). Decision Assistance in Risk Assessment-Monte Carlo Simulations. *InformaticaEconomica*, *16*(4), 86-92.

[11] Tamjidyamcholo, A., & Al-Dabbagh, R. D. (2012). Genetic algorithm approach for risk reduction of information security. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *1*(1), 59-66.

[12] Behnia, A., Rashid, R. A., & Chaudhry, J. A. (2012). A survey of information security risk analysis methods. *SmartCR*, *2*(1), 79-94.

[13] García, D. F., &Fernández, A. (2013, August). Effective Methodology for Security Risk Assessment of Computer Systems. In *Proceedings of World Academy of Science, Engineering and Technology* (No. 80, p. 44). World Academy of Science, Engineering and Technology (WASET).

[14] Kiran, K. V. D., Reddy, D. L., &Haritha, N. L. (2013). A Comparative Analysis on Risk Assessment Information Security Models. *International Journal of Ccomputer Applications*, *82*, 41-46.

[15] Ahmad, E. W., Fallouh, G., &Idris, N. B. (2013). A Novel Approach to Design Quantitative Method for ICT Security Assessment.

[16] Hassan, A. (2013). Information Security Management for Strategic and Effective Implementation of e-Management in the Governmental Institutions in Gaza. Lap Lambert Academic Publishing.

[17] Bojanc, R., &Jerman-Blažič, B. (2013). A quantitative model for information-security risk management. *Engineering Management Journal*, *25*(2), 25-37.

[18] Lee, Z. J., & Chang, L. Y. (2014). Apply fuzzy decision tree to information security risk assessment. *International Journal of Fuzzy Systems*, *16*(2), 265-269.

[19] Ghazouani, M., Faris, S., Medromi, H., &Sayouti, A. (2014). Information Security Risk Assessment--A Practical Approach with a Mathematical Formulation of Risk. *International Journal of Computer Applications*, *103*(8).