Journal of Theoretical and Applied Information Technology
15th July 2016. Vol.89. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FUZZY ORIENTED RISK ASSESSMENT IN ENTERPRISE INFORMATION SYSTEMS

[1]G.MANI BHARAT, [2]Dr. M.SEETARAMA PRASAD

[1]Student., Department of Computer Science & Engineering, KL University,Vaddeswaram,INDIA
[2]Professor., Department of Computer Science & Engineering, KL University,Vaddeswaram,INDIA
E-mail: [1]manibharat1379@gmail.com, [2]msrprasad@kluniversity.in

ABSTRACT

Records in corporation infrastructure is greater complex and face a troubles with threat in employer property increasing workload performance in real time packages. therefore evaluation of the process identity, and mitigation of records protection in agency applications may obtain promising concept in facts security. Traditionally Quantitative statistics protection analysis method proposed for business enterprise packages in real time facts safety. Specific technique identifies the chance-vulnerability pair liable for a threat and computes a chance element similar to every protection property for each asset. Because of this an assault on one asset can be propagated through the network and threaten an organization's maximum valuable belongings. Linguistic terms are used by the experts to represent assets values, dependencies and frequency and asset degradation associated with feasible threats. Computations are based totally on the trapezoidal fuzzy numbers associated with these linguistic terms.

Key words: *Information Systems, Risk Analysis, Fuzzy Information Analysis, Enterprise Information Security.*

1. INTRODUCTION

The rate and scale of statistics systems is increasing day by day. pc networks have emerge as ever pervasive and have made lifestyles easy and fast, however along side that it gives upward push to numerous threats to facts systems. A system containing data assets, whilst associated with the out of doors world, is exposed and is liable to assaults that might purpose lack of crucial records and sources. assaults to belongings are as a result of threats which have the capability to take advantage of the vulnerabilities associated with an asset. In great, assets serve the enterprise desires of an employer and any damage to these property in any shape reasons hazard and is of remarkable problem to that commercial enterprise enterprise. This requires a scientific technique to evaluate facts safety dangers and expand an appropriate safety method. officially, danger may be described because the functionality harm delivered on if a particular chance exploits a particular vulnerability to reason harm to an asset. hazard assessment is defined because the machine of identifying protection risks and determining their magnitude and impact on an organization [9, 10]. Threat analysis ought to be completed prior to any software, gadget, challenge, or way going into production.

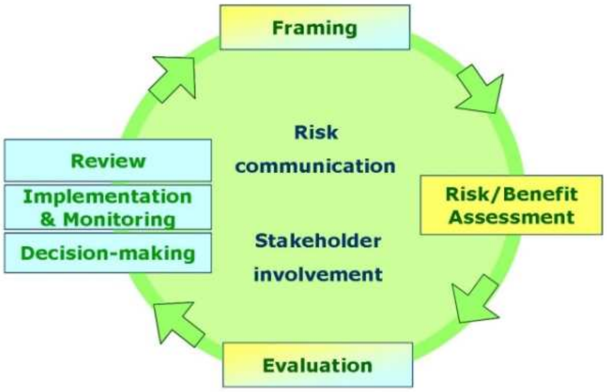

Figure 1: Risk Analysis With Proceedings Of Real Time Organization.

As shown in above figure 1 danger verbal exchange achieves stakeholder assessment in business enterprise. A quantitative threat evaluation technique, that identifies risks related to an asset, has been proposed. The concept is to divide a tough and speedy of belongings into three particular chance zones specially immoderate, medium and espresso danger location. For high-threat property, management can also set up excessive fee infrastructure to guard an asset. For medium-chance property, manage may additionally moreover use low price tools or study safety guidelines, guidelines and processes to defend the asset. control may additionally decide now not to invest a few element for property at low-threat. The proposed methodology will assist businesses to align themselves with facts safety pleasant practices and requirements. Technological tendencies and the time-venerated internet get admission to has induced an growth in device vulnerabilities. consequently, ISs want to be analysed so that it will risk minimization by using way of well-planned movements to guard information, techniques and offerings from feasible threats. Threats range from act of terrorism, enterprise espionage, and so forth., or maybe a easy accidental human error with the useful resource of an operator.

The asset dependencies are normally represented in phrases of possibilities, signalling how in all likelihood the failure of an asset is to affect another. often only a few factors (terminal assets), generally statistics or services, account for the whole price of an organization's belongings. The cost of these assets is transferred to different assets thru the installed dependency relations. therefore, non-terminal property have no intrinsic values; they collect their value from terminal belongings. In this paper, we attention on the second degree, evaluation. assets are the IS or associated sources, necessaryfor an employer's accurate operation and for carrying out the desires set by way of way of its manager. belongings may be facts, programs, software, facilities, hardware, services.. In this paper we advocate a fuzzy chance analysis in IS as a option to those deficiencies.

2. RELATED WORK

Some big data safety hazard evaluation methodologies are as follows [5]:

(a) OCTAVE approach [1] which defines the crucial additives of a context-driven facts protection threat assessment. This technique lets in an agency to make statistics-safety alternatives based totally mostly on dangers to confidentiality, integrity, and availability of important facts generation assets. the usage of a 3-phase approach, OCTAVE examines organizational and generation troubles to accumulate a complete picture of the statistics safety desires of an organization. A crew is established inside an employer to perform threat analysis. The organization identifies the assets which is probably vital for the organisation. Interasset dependencies are also taken into consideration. The technique is nonlinear and additionally iterative in nature. because of its iterative nature, there are numerous remarks loops in this technique.

(b) "Ten Step procedure" [7] defines ten exactly described sports for risk assessment. the stairs encompass development of Scope declaration, Assembling a competent crew, identification of Threats, Prioritization of Threats, Prioritization of Loss effect, Calculation of danger thing, identification of Safeguards, value- gain assessment, rating of Safeguards in priority Order, and practise of hazard assessment file. but, this system does not bear in thoughts vulnerabilities explicitly.

Table 1: Risk Analysis Events With Different Tools

Risk Assessment Methods and Tools	Elements Considered for Risk Assessment	Follows Quantitative Methodology? (Y/N)
OCTAVE	Security Parameters	Partial
Ten step Process	Threats	N
FRAAP	Threats	N
COBRA	Secuirty Threats	Y

desk 1 provides a comparative summary of the hazard assessment methodologies and equipment described above. None of these methodologies cater to the needs of statistics security requirements and first-class practices. furthermore, every technique is desirable to the wishes of apecific enterprise or fashion of business enterprise.

(c) Facilitated chance evaluation and evaluation way (FRAAP) is a qualitative threat evaluation method that tries to discover dangers in terms of their consequences on enterprise strategies or project of the business organization. It does no longer try to attain unique numbers for danger hazard or loss estimates. It focuses on identifying chance-inclined areas and suitable controls to mitigate them. An expert acts because the facilitator for the duration of the entire technique. considering, FRAAP relies intently on inputs from an professional, it suffers the dangers that most qualitative methodologies have – lack of consistency in hazard values.

3. QUANTITATIVE ANALYSIS BASED RISK IDENTIFICATION

Quantitative evaluation approach computes a danger difficulty fee for each asset.

Hazard Difficulty: danger factor [RF] related to an asset is described as a function of asset price and its protection situation. This parameter identifies the threat concerned with an asset and, relying on this rate, an asset is decided to be at high, medium or low hazard..

$$RiskFactor(RF) = \dagger(AV, SC)$$

Where in, AV is asset rate and SC is safety situation (defined later) of an asset. Asset rate: Asset charge [AV] of an asset is defined as a characteristic of protection, commercial organisation and legal and contractual requirements (described in section 3) related to an asset. it's miles a graded parameter and its value is obtained on a scale of one to five..

$$AssetValue = \square(SR, BR, LR)$$

where, SR is protection requirement, BR is commercial enterprise requirement and LR is criminal requirement. those 3 parameters are calculated as follows:

$$\mathrm{SR} = (\mathrm{C} + \mathrm{I} + \mathrm{A} + \mathrm{Au} + \mathrm{Nr})/5, \text{ if Au } \ 0, \text{ Nr } 0;$$
$$(\mathrm{C} + \mathrm{I} + \mathrm{A} + \mathrm{Au})/4, \text{ if Au } 0, \text{ Nr} = 0;$$
$$(\mathrm{C} + \mathrm{I} + \mathrm{A} + \mathrm{Nr})/4, \text{ if Au} = 0, \text{ Nr } \ 0;$$
$$(\mathrm{C} + \mathrm{I} + \mathrm{A})/3; \text{ if Au} = 0, \text{ Nr} = 0.$$

BR = Li

LR = Lr

Asset price [AV] is calculated as AV = ┐ *SR+ └ *LR+ ┘ *BR, ┐ +└ +┘ =1, if LR │ zero; ┐ *SR + └ *BR, ┐ +└ =1, if LR = zero. (four)

proper right here, , , and are relative weights which can be assigned to safety, industrial business enterprise, and crook requirements, respectively. it may be mentioned that man or woman components of SR were assigned equal weights (tested in Eq. 1). However, if needed, these components may be assigned relative weights primarily based totally on priorities of an business enterprise. as an instance, a army employer may also choose out to attach extra significance to confidentiality requirements in comparison to the opportunity security parameters; consequently, weights may be custom designed as a end result.

Thinking about that protection requirement is the maximum important determinant for computing safety hazard, higher weight need to be assigned to it. Enterprise requirement and legal and contractual requirement for an asset depend upon the form of business enterprise, its assets and the way they are used. consequently, the weights for calculating asset cost AV may be adjusted depending on the unique requirements of an employer..

4. FUZZY BASED RISK ASSESSMENT

MAGERIT defines the rate of an asset due to the fact the losses that would be sustained if the respective asset is not any longer available. Those may be losses of cash, user self assurance, the organizational prestige. Assets are generally evaluated considering the following 5 components

• Confidentiality. How an lousy lot damage would it no longer purpose if the asset is disclosed to someone it have to now not be? that may be a everyday facts inspection.

• Integrity. How lots harm would it not not purpose if the asset is broken or corrupt? that could be a normal information inspection. statistics may be manipulated, be completely or partially false, or even missing.

• Authenticity. How lots damage wouldn't it cause if we do not precisely recognize who has completed what? this is a fashionable services (consumer authentication) and statistics (authenticity of the individual gaining access to information to put in writing or read) inspection.

• Traceability. How plenty harm would it not reason if it is not stated for whom the company is being provided?, i.e. who does what and whilst? How an lousy lot damage would it motive if it isn't identified who accessed what statistics and what they did with them?

• Availability. How an awful lot harm would it not cause if the asset is not to be had or cannot be used? this is a everyday offerings inspection. handiest the terminal assets have an associated price for the above additives. the opposite belongings acquire price from terminal belongings on the idea of dependency relationships. We once more use the set of linguistic phrases that represent trapezoidal fuzzy numbers to represent uncertainty whilst valuating the terminal assets.

Allow us to denote property through evj = (evj(1) ,evj(2) ,evj(three) ,evj(4) ,evj(five)), wherein evj(i) is a linguistic time period assigned via way of an professional for the ith price component in asset Aj . If we denote by manner of TAS the terminal asset set, then the fee of asset Aj with admire to terminal.

Subsequent, we test threats and estimate signs of the effect on and danger to belongings. A chance is an event that may trigger an incident in our enterprise, inflicting damage or intangible fabric loss to the belongings, and an assault is any planned motion geared toward violating the IS protection mechanisms. MAGERIT shows threat evaluation measures: degradation, the harm that the hazard can motive to the asset, and frequency, how regularly the chance materializes. we can once more use fuzzy linguistic terms in place of possibilities and opportunities to represent degradation and frequency. A risk is a vector −→ecu = (eD, ef) whose additives are degradation and frequency.

Threat assessment aids in growing a protection approach and gives the idea for setting up a rate-powerful protection software program that minimizes the effects of danger. Preparation of the risk evaluation document marks the completion of the chance analysis technique or cycle. After the record is forwarded to this device supervisor and regularly occurring, the planning approach vital to establish the technical and procedural defensive security functions diagnosed within the record want to begin. The a hit implementation of a safety program depends on manipulate involvement. This involvement includes planning for the protection of facts belongings. The planning manner identifies dreams, establishes priorities, implements targets, obtains resources, and secures determination to the safety plan, which includes a contingency plan for data belongings offerings resumption.

5. RISK ANALSYS WITH FUZZY EXPERIMENATAL EVALUATION

Similarity function is required to partner the following trapezoidal fuzzy variety with an element in the linguistic time period set. This function can also be used at any step of the method to derive the linguistic phrases associated with the respective trapezoidal fuzzy numbers output to represent dependencies, accrued values... severa authors have proposed terrific similarity capabilities, which can be based at the centroid of a fuzzy wide variety and the space among the additives of the bushy numbers, see (Lee, 1999; Chen and Chen 2001, 2007). Finally, a extra latest similarity function became proposed in (Xu et al., 2010) and in assessment with the concept mentioned in (Chen and Chen, 2007). We use the feature proposed in Vicente, Mateos and Jim´enez (2012), which considers every other parameter which include the ratio a few of the commonplace place and the joint area under the club skills of trapezoidal fuzzy numbers. Moreover, we use the gap l¥ among centroids when you consider that using distances with non-rectangular spheres is inconsistent with the intuitive belief of similarity.

An implementation plan and a agenda for instituting the proposed shielding protection measures need to be advanced. furthermore, methods to put into effect the goals have to be identified. The plan should assign security duties to control; to information protection feature personnel; and to the proprietors, customers, and custodians of statistics. The fulfillment of the safety software relies upon on the right venture of security obligations. The risk assessment manner need to be completed with enough regularity to make certain that the technique to threat management is a realistic response to the modern-day risks related to its facts belongings. Consequently, the safety plan may also require reassessment and meantime updates must large changes in protection troubles stand up.

$$\text{S(A,B)=1-w}_1(1-\frac{\int_0^1 \mu_{A\cap B}(x)dx}{\int_0^1 \mu_{A\cup B}(x)dx})-w_2\frac{\sum \| ai-bi \|}{4}$$

$$-w_2\frac{\sum | ai-bi |}{4}-w_3\int_{\infty}[(X_A,Y_A),(X_B,Y_B)],$$

where w1+w2+w3 = 1, (XeA,YeA) and (XeB,YeB) are the centroids of eA and eB, respectively, i.e.

$$X_A = Y_A(a3+a2)+(1+Y_A)(a4+a1)and$$

$$Y_A=\{\begin{matrix} \frac{\frac{a3-a2}{a4-a1}+2}{6} & ifa4-a1\neq 0 \\ 1/2 & ifa4-a1=0 \end{matrix}$$

1¥((x1,y1), (x2,y2)) = max y1−y2 .

observe that w1, w2 and w3 represent the relative significance of the 3 elements considered within the similarity feature. Analysts will assign the values that satisfactory suits their own model.

6. CONCLUSION

We have evolved a fuzzy threat evaluation model for data systems that conforms to international requirements, specially the MAGERIT method. The version is an development in this and different existing methodologies as it includes uncertainty approximately the assessments with the resource of linguistic terms, that have associated trapezoidal fuzzy numbers. The proposed method makes computations on the premise of trapezoidal fuzzy numbers to build up dependencies amongst property and asset valuations and to determine impacts and risk from the threat degradation and frequency, respectively. Furthermore, similarity skills may be used at any step in the method to derive a linguistic time period for the trapezoidal fuzzy range output.

REFERENCES

[1] Jaya Bhattacharjee, Anirban Sengupta, “A Two-Phase Quantitative Methodology for Enterprise Information Security Risk Analysis” In *Proceedings of First International Conference on Information Systems Security* (Kolkata, India, 2005). ICISS 2005. LNCS 3803, Heidelberg, Germany, 328 – 331.

[2] Eloy Vicente, Antonio Jim´enez and Alfonso Mateos,” A Fuzzy Approach to Risk Analysis in Information Systems”, CONFERENCE PAPER · FEBRUARY 2013.

[3] *CORAS: A platform for risk analysis of security critical systems* - http://www2.nr.no/coras/

[4] *CRAMM: Information Security Risk Assessment Toolkit* - http://www.cramm.com

[5] *enisa: European Network and Information Security Agency* - http://rm-inv.enisa.europa.eu/rm_ra_methods.html

[6] Mazumdar, C., et. al. 2007. Enterprise Information Security Risk Analysis: A Quantitative Methodology. In *Proceedings of the National Workshop on Software Security* (New Delhi, India, 2007), S. I. Ahson and M. Mehrotra, Ed. NWSS 2007. I. K. International Publishing House Pvt. Ltd., New Delhi, India, 1-12.

[7] Peltier, T. R. 2010. *Information Security Risk Analysis*. Third Edition, Auerbach Publications, USA.

[8] Sengupta, A., et. al. 2005. A Web-Enabled Enterprise Security Management Framework Based on a Unified Model of Enterprise Information System Security: (An Ongoing Project Report). In *Proceedings of First International Conference on Information Systems Security* (Kolkata, India, 2005). ICISS 2005. LNCS 3803, Heidelberg, Germany, 328 – 331.

[9] Stoneburner, G., et. al. 2002. *Risk Management Guide for Information Technology Systems*. NIST Special Publication 800-30, MD, USA.

[10] The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC). 2005. *ISO/IEC 27002:2005, Information technology – Security techniques - Code of practice for information security management*. Edition 1. Switzerland.

[11] The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC). 2009. *ISO/IEC 31010:2009, Risk management — Risk assessment techniques*. Edition 1. Switzerland.

[12] The International Organization for Standardization, The International

Electrotechnical Commission (ISO/IEC). 2011. *ISO/IEC 27005:2011, Information technology – Security techniques - information security risk management*. Edition 1. Switzerland.

[13] *Unified Modeling Language* - http://www.uml.org/

[14] Vorster, A. and Labuschagne, L. 2005. A Framework for Comparing Different Information Security Risk Analysis Methodologies. In *Proceedings of the Annual Research Conference of the South African Institute of Computer Scientists* (South Africa, September 20-22, 2005). SAICSIT 2005. ACM, New York, NY, 95–103.

[15] Alberts, C. and Dorofee, A. (2005). *OCTAVE-s Method Implementation Guide Version 2.0*. Pittsburgh: Canergie Mellon University. Chen, S.-J. and Chen, S.-M. (2001). A New Method to Measure the Similarity between Fuzzy Numbers. *Proceedings of the 10th IEEE International Conference on Fuzzy Systems*, 208-214.

[16] Chen, S.-J. and Chen, S.-M. (2007). Fuzzy Risk Analysis Based on the Ranking of Generalized Trapezoidal Fuzzy Numbers. *Applied Intelligence*, 26, 1-11. CCTA *Risk Analysis and Management Method (CRAMM), Version 5.0*. London: Central Computing and Telecommunications Agency (CCTA), 2003. ISO/IEC 17799:2005, *Information technology - Security techniques - Code of practice for information security management*. Geneva: International Organization for Standarization.

ISO/IEC 27005:2011, *Information technology – Security techniques - Information security risk management*. Geneva: International Organization for Standarization.

[17] Lee, H.S. (1999). An Optimal Aggregation Method for Fuzzy Opinions of Group Decision. *Proceedings of the 1999 IEEE International Conference on Systems, Management and Cybernetics*, 314-319.

[18] L´opez Crespo, F., Amutio-G´omez, M.A., Candau, J. and Ma˜nas, J.A. (2006a). *Methodology for Information Systems Risk. Analysis and Management (MAGERIT version 2). Book I-The Method*. Madrid: Ministerio de Administraciones P´ublicas.

[19] L´opez Crespo, F., Amutio-G´omez, M.A., Candau, J. and Ma˜nas, J.A. (2006b). *Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2). Book II-Catalogue of Elements*. Madrid: Ministerio de Administraciones P´ublicas.