20 Integrated Methodology for Information Security Risk Assessment

Ping Wang and Melva Ratchford

Abstract

Information security risk assessment is an important component of information security management. A sound method of risk assessment is critical to accurate evaluation of identified risks and costs associated with information assets. This paper reviews major qualitative and quantitative approaches to assessing information security risks and discusses their strengths and limitations. This paper argues for an optimal method that integrates the strengths of both quantitative calculation and qualitative evaluation for information security risk assessment.

Keywords

Security • Risk • Assessment • Qualitative • Quantitative

20.1 Introduction

Information security risk management is "the process of identifying, assessing, and reducing risks to an acceptable level and implementing the right mechanisms to maintain that level of risk" [15]. Therefore, risk assessment is a critical component in the information security risk management process. Effective risk management is dependent upon a sound risk assessment, also known as risk analysis, which is a process for identifying and evaluating risks [7]. Accurate evaluation of the risks or potential losses associated with the vulnerabilities of information assets is essential to the development of effective risk control process and protection strategies.

A risk is the possibility of an adverse event that would reduce information and business asset [4]. Blakley et al. also pointed out that every information security risk has a cost which can be more or less precisely quantified [4]. Therefore, maximum accuracy in quantifying the cost or loss related to the security risks is certainly an important attribute for any risk analysis methodology. There are two general approaches to risk assessment: quantitative approach and qualitative approach. The quantitative approach uses numeric data, formulas, and calculations to obtain an objective measure of risks. A typical mathematical formulation of risk uses a lower level of granularity of threat and probability to determine an asset's value, exposure, frequency and existing protection measures [6]. The qualitative approach is more subjective and uses expert opinions and perceptions on the probability and impact of a risk to determine the risk level. Both quantitative and qualitative approaches have their own strengths and limitations. For a typical risk assessment, an appropriate approach or methodology should be selected based on the business mission and assessment needs. In addition, critical assets and relevant vulnerabilities and threats need to be identified. Various controls for mitigating the risks need to be identified and evaluated in terms of effectiveness and costs. A cost-benefit analysis (CBA) should be included to support any recommendations of controls.

There are various risk analysis and assessment methodologies currently available. These methodologies are

P. Wang (✉)
Robert Morris University, Pittsburgh, PA, USA
e-mail: wangp@rmu.edu

M. Ratchford
University of Maryland University College, Adelphi, MD, USA
e-mail: melva.ratchford@gmail.com

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent
Systems and Computing 558, DOI 10.1007/978-3-319-54978-1_20

primarily quantitative or qualitative in nature addressing various dimensions of information security risks, and an organization often faces the challenging task of adopting the optimal or most appropriate methodology. The common goal of risk assessment methodologies is to reach the estimate of overall risk value and the appropriateness of the methodology should fit the needs of the organization [14]. This paper is to briefly review the major approaches to information security risk assessment and propose an optimal and integrated methodology.

20.2 OCTAVE Method

A widely known qualitative methodology for assessing information security risk is the OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM}) method. OCTAVE is a risk-based strategic assessment and planning technique developed by the CERT Coordination Center at Carnegie Mellon University Software Engineering Institute (SEI). OCTAVE method is driven by operational risks and security practices and uses three phases and sub-processes and task activities to build a comprehensive picture of organizational information security needs [1].

The OCTAVE approach has several positive features, including self-direction, flexibility, and comprehensiveness [2]. The method is self-directed, which means that a small internal team can take the lead in analyzing the organizational security needs while incorporating the knowledge of a wide range of employees. It is flexible with different versions and can be customized to fit the needs of different types and sizes of organizations. It is also comprehensive because it focuses on both strategic and organizational risks as well as practical operational security management and technology issues.

However, the end result of OCTAVE risk analysis uses subjective and relative ranking values (high, medium, low) and a descriptive risk-level matrix for risk impact and probability determination. While the relative and categorical rankings may be simple and flexible for individual organizations to use and define, they lack mathematical calculations and quantitative results needed for comparing risk differences [14]. Thus, it would be difficult to use the OCTAVE results as accurate parameters for supporting cost-benefit analysis and decision-making regarding risk control investments and activities.

20.3 CORAS Method

Another qualitative methodology for information security risk assessment is CORAS (Construct a platform for Risk Analysis of Security Critical Systems). CORAS was a framework for model-based risk assessment of security-critical systems developed under the Information Society Technologies program sponsored by the European Union. The CORAS methodology uses UML (Unified Modeling Language) diagrams to represent relationships and dependencies between users and the working environment and the final outcome of risk analysis and risk management decisions are based on the UML class diagrams involving each asset [11].

The major strengths for the CORAS approach include its incorporation of input from and communication among diverse parties and stake-holders as well as improved asset specification and efficiency in the organizational risk analysis process. However, like the OCTAVE methodology, CORAS is a qualitative approach and does not use any precise mathematical calculations but uses an expected value matrix with subjective rankings to determine the expected value of a security risk. The CORAS method is simple and efficient to use but is subjective and lacks accuracy and specificity in risk values.

20.4 IS Risk Analysis Method

Traditional qualitative risk assessment methodologies provide subjective and relative results for risk impact and are not adequate for cost-benefit decision support. To address this limitation of qualitative methods, the IS (information system) Risk Analysis method was proposed based on a business model [13]. The IS Risk Analysis methodology is a systematic quantitative model with four sequential stages which determine the importance levels and valuations of various business functions and IS assets. Mathematical formulas are used to calculate the annual loss expectancy (ALE) for each threat occurrence and organizational disruption.

The ALE calculation in the IS Risk Analysis method is more comprehensive than conventional understanding of loss. The loss of asset due to each threat includes not only the asset replacement cost but also the income loss, the probability of the threat occurrence, and the relative importance of the asset from the viewpoint of the operational continuity. Most importantly, the risk assessment end result is a tangible quantitative monetary value that can be used for making risk management decisions. However, the four stages of the method involve extensive mathematical calculations and may not be simple enough to attract wide participation from management and staff [14].

20.5 ISRAM Method

Another major quantitative method for information security risk analysis is the survey-based ISRAM (Information Security Risk Analysis Method) developed by Karabacak and

Sogukpinar [9]. ISRAM uses a 7-step process including two surveys among managers and staff on the probability and consequence for each of the identified security vulnerabilities. The survey results are numerically represented and used in a formula to calculate the final risk value.

Karabacak and Sogukpinar demonstrated the ISRAM approach with a case study on computer virus infection risks. ISRAM does provide quantitative and objective risk values for supporting risk management decisions. At the same time, the survey instrument used in the ISRAM model includes subjective but numerical evaluations from managers and staff in the operational community. In addition, the survey questions and weight values are customizable with no rigid frames to fit to organizational and business needs. Karabacak and Sogukpinar also claimed the advantage of simplicity and ease-of-use for the method. However, the 7-step process of ISRAM needs extensive preparation and the mathematical formulas are complex and daunting to many potential participants [14].

20.6 Proposal: Integrated Method

The review of the information security risk assessment methodologies presented above reveals strengths and limitations in both qualitative and quantitative approaches. It is important for an organization to adopt an optimal risk analysis method that is accurate in providing end results and customizable according to organizational needs. To facilitate accurate and effective information risk assessment, it is also necessary to identify indirect and hidden risks and costs and compare and analyze various information security risk assessment models and evaluate and prioritize the criteria for selecting effective risk assessment models [3, 8].

Even for qualitative risk evaluation methods, quantifiable and accurate data should be a pre-requisite especially for the area of information security risk analysis [4]. Therefore, an optimal information security risk analysis methodology should integrate the strengths of both qualitative and quantitative methods.

The Risk Management Guide for IT Systems (SP 800–30) published by NIST (National Institute of Standards and Technology) under the U.S. Commerce Department provides an example effort for optimized and integrated direction toward assessing security risks and impacts [10]. The NIST guide uses a qualitative Risk-Level Matrix and subjective and descriptive variables (high, medium, low) to reference risk levels. However, it uses a numeric and quantifiable value to translate the subjective evaluation of the probability of exploitation of a specific vulnerability. The NIST guide also acknowledges the limitations of the subjective evaluations and emphasizes that risk and impact analysis should consider the advantages and disadvantages of both qualitative and quantitative methods and the additional factors of frequency, cost, and weight of the risk impact for a particular vulnerability [12].

Whitman and Mattord provide an example of a security risk assessment method that integrates both qualitative and quantitative strengths [16]. In the Whitman and Mattord risk assessment model, the equation for determining the risk is: The total risk value *equals* the likelihood of vulnerability occurrence *times* the value of the information asset, *minus* percentage of risk mitigated by current controls, *plus* an element of uncertainty of current knowledge of the vulnerability. It is especially important to include the uncertainty cost factor in the equation since "it is not possible to know everything about every vulnerability" [16]. This method provides numeric and quantifiable end results for risk assessment and management while using the subjective likelihood rating of vulnerability recommended by NIST.

However, the asset loss calculation still reflects the limited traditional concept of annual loss expectancy (ALE). As an improvement for the ALE concept, Bodin, Gordon, and Loeb (2008) introduced the new metrics of expected severe loss and standard deviation of loss in addition to ALE in calculating the total risk value. The expected severe loss is the magnitude of the loss that jeopardizes the organizational survivability [5]. The standard deviation of loss (the square root of the variance of loss) scientifically measures the dispersion of risks and losses. The weighting of each loss parameter can be customized by individual organizations.

20.7 Conclusion

In conclusion, an optimal methodology for information security risk assessment should integrate strengths from both qualitative and quantitative methods to provide accurate and reliable risk data for risk management decision making. The integrated methodology should include the strategic, practical, and customizable phases and processes from the OCTAVE method while incorporating the survey instruments used by the ISRAM method into its processes for diverse and quantifiable input on risk evaluations. In identifying critical assets and their behaviors, the object-oriented UML modeling technique from the CORAS method can be used to improve asset specification. In addition, the risk scores for assets should follow the NIST recommendation that is subjective but numeric and quantifiable. Finally, the total risk value calculation should include ALE, expected severe loss, standard deviation of loss, minus risk mitigation by current controls, and plus uncertainty cost.

References

1. Alberts, C., & Dorofee, A. (2002). *Managing information security risks: The OCTAVE approach*. Boston: Addison Wesley Longman Publishing Co., Inc..
2. Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). Introduction to the OCTAVE approach. Retrieved from http://www.cert.org/octave/pubs.html
3. Anderson, R., & et al. (2013). Measuring the cost of cybercrime. *The Economics of Information Security and Privacy*. Springer.
4. Blakley, B., McDerMott, E., & Geer, D. (2002). *Information security is risk management. NSPW'01, September 10–13th, 2002, Cioudcroll, New Mexico,* 97–104.
5. Bodin, L. D., Gordon, L. E., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM, 51*(4), 64–68.
6. Ghazouani, M., et al. (2014). Information security risk Assessment — A practical approach with a mathematical formulation of risk. *International Journal of Computer Applications, 103*(8), 36–42.
7. Gibson, D. (2015). *Managing risk in information systems* (2nd ed.). Burlington: Jones & Bartlett Learning.
8. Kiran, K. V. D., et al. (2013). A comparative analysis on risk assessment information security models. *International Journal of Computer Applications, 82*(9), 41–47.
9. Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. *Computer & Security, 24*(2005), 147–159.
10. NIST. (2012). *"Guide for Conducting Risk Assessments*" *(NIST SP800–30 Revision 1) by NIST (2012)*. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
11. Stolen, K., den Braber, F., Dimitrakos, T., Fredriksen, T., Gran, B. A., Houmb, S., et al. (2002). *Model-based risk assessment – the CORAS approach*. Retrieved from http://www.nik.no/2002/Stolen.pdf
12. Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems: Recommendations of NIST*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
13. Suh, B., & Han, I. (2003). The IS risk analysis based on a business model. *Information & Management, 41*(2003), 149–158.
14. Vorster, A., & Labuschagne, L. (2005). A framework for comparing different information security risk analysis methodologies. Proceedings of SAICSIT 2005, pp. 95–103.
15. Wang, J. A. (2005). Information security models and metrics. *Proceedings of the 43rd ACM Southeast Conference, March 18–20, 2005, Kennesaw, GA*. 178–184.
16. Whitman, M. E., & Mattord, H. J. (2008). *Management of information security* (2nd ed.). Boston: Thomson Course Technology.