International Journal of Computer Applications Technology and Research
Volume 6–Issue 6, 242-244, 2017, ISSN:-2319–8656

Efficacy of OCTAVE Risk Assessment Methodology in Information Systems Organizations

Muhammad Asif Khan
Department of Information Systems
College of Computer Science and Engineering
Taibah University, Madina al Munawwara, Saudi Arabia

Abstract: With the increasing use of computers in business information security has also become a key issue in organizations. Risk assessment in organizations is vital in order to identify threats and take appropriate measures. There are various risk assessment methodologies exist which organizations use for risk assessment depending the type and need of organizations. In this research OCTAVE methodology has been used following a comparative study of various methodologies due to its flexibility and simplicity. The methodology was implemented in a financial institution and results of its efficacy have been discussed.

Keywords: risk; OCTAVE; information systems; security; risk assessment; methodology

1. INTRODUCTION

Information organizations have growing concerns of security of information and associated assets. Now information security is considered the key and prime issues worldwide. Information security is a set of procedures and processes, technology and people which aim to protect assets of organizations [1]. In organizations there are various risks and companies face a major issue that how to evaluate those risks in order to use security controls for removing or mitigating the identified risks [2]. There is no standard methodology or procedure which can be used by organizations. There are numerous risk assessment methods and frameworks [3] and organizations aspiring for security of information need to compare different methodologies and select the best method that suits to their needs. In results of risk assessment organizations measure the severity of risks and develop security controls in order to mitigate the loss and gain maximum benefit from the investment done on security measures. Generally, following identification of risks organizations determine the value of threat, its probability of occurrence and impact the threat may have in organization. The severity of risk can be determined by combining threat occurrence and its impact which can be achieved by applying qualitative, quantitative or both methods at the same time [4].

Organizations may face security threats by various means such as information exposed to hackers on internet, malicious and unscrupulous employees, and breach in physical security. Financial organizations experience financial damage in result of security breach that is sometimes unnoticed due to insignificant security events [5]. As stated earlier, there is no standard methodology or procedure which can be adopted by organizations to determine risk to information security, organizations usually chalk out detailed steps for risk assessment. The proper risk assessment planning helps staff assigned for risk assessment for acting effectively and in a systematic way. In order to assess risks in organizations first risks to the most valuable information assets are prioritized and then level of severity of threat to the assets is evaluated. There are generally two type of risk assessment conducted namely qualitative assessment and quantitative assessment.

A qualitative assessment is the one in which descriptive or relative scale is used to determine probability of occurrence of a threat to an information asset. The evaluators of information assets assess possible threats by drawing some vulnerable scenarios and assign a descriptive scale rather than a numeric value. For example, probability of risk occurrence in a component can be defined as ‘high’, ‘medium’ or ‘low’. This assessment is simple and non-technical people can also be involved in the assessment.

A quantitative assessment uses a numeric value to indicate probability of risk occurrence to an information asset. All risk threat elements are quantified. A probability of occurrence of a risk event is indicated using a numeric value as 35% or 60% etc. Since this method is based on numeric values the calculations may become more complex. This assessment is difficult and employees may find intricacies in understanding it.

2. RISK ASSESSMENT METHODOLOGIES

There are various risk assessment methodologies used by different organizations depending on the type and need of organizations. Some methodologies require large enterprises and experienced staff to use them as they are quite sophisticated to be used. Most of the methodologies are commercially developed, therefore, unavailable to public except some for marketing purpose. An organization needs to use a methodology for risk assessment usually intends to compare different methodologies before the right one cold be selected. But investment on purchasing different methodologies for comparison purpose is not viable. Since documentation and presentations on different methodologies are available comparison, most of the time comparison is made through such material. Table 1 shows a list of risk assessment methodologies that are commonly used in organizations

Table 1. Risk assessment methodologies

Methodology	Description
Asset Audit	In order to determine whether assets of a company have a potential threat. It also determines likelihood of occurrence of a threat and impact of threat
CORAS	A qualitative model-based methodology consists of four diagrams – an extension of UML. It requires expert knowledge to use for risk assessment
CRAMM	This is qualitative methodology that focuses on assets and valuation. Following valuation of assets likelihood of threat is determined. It requires experts to use
OCTAVE	A qualitative simple methodology that can be used by knowledgeable small team of business and IT people. It is not driven by technology but practices of security and risk which propagate main information of security
NIST	A qualitative or quantitative methodology that is cost effective and quick in assessing security within organizations via survey instruments
Risk IT	A complementary part of COBIT framework developed by ISACA. It provides guidelines for IT security as well as risk assessment which cannot be used freely without using the framework

It can be observed that all risk assessment methodologies have some disparities in terms of scope or application. Some of them require expertise and thorough knowledge whereas some methodologies work in combination of generic framework of risk assessment.

2.1 OCTAVE methodology

Operationally Critical Threat, Asset, Vulnerability and Evaluation (OCTAVE) methodology was develop at Carnegie Mellon University, USA [6]. This methodology is used in small to medium organizations. It can be tailored according to an organization environment. Using the methodology firms can reduce overhead cost spent on training and knowledge development that are required for risk assessment. This methodology is comprised of three phases and each phase consists of a number of processes.

2.1.1 Phase 1 - Build asset profiles

In this first phase all the important assets, prevailing security practices and vulnerabilities in organizations are identified. Also staff knowledge about assets, their vulnerabilities and current security strategies are identified. Based on such information most important vulnerable assets are sorted out.

2.1.2 Phase 2– Identify infrastructure vulnerabilities

In the second phase infrastructure of the organization is evaluated in order to determine technological vulnerabilities which could harm important assets. The components which are most critical are further evaluated and technological weaknesses are detected.

2.1.3 Phase 3 – Develop security strategy and plans

In the third phase security risks in the assets identified in the previous phase are mitigated if not removed completely. In order to evaluate impact of threats to the assets criteria are developed which in turn gives risk profile to each asset. Finally, a strategy for protection of assets is developed and an approval is requested from the management.

3. EFFICACY OF OCTAVE METHOD

As discussed earlier OCTAVE methodology is a simple that can be used with small team of knowledgeable employees within an organization. In order to determine the risk assessment in a financial organization in Saudi Arabia this method is used and for this purpose all three phases of the methodology were implemented step by step. To start with the OCTAVE methodology initially two teams were formed within the financial institution i.e. one from the business department and another from IT department. In both the teams members were knowledgeable in their respective fields and capable of giving answers to the questions related to security and vulnerability. To start with the research study different sessions, discussions and interviews were conducted with both the teams in order to know vulnerable assets and current strategy to protect them. After collecting information critical assets with vulnerability were evaluated and further detailed discussions were held with the management in order to ensure criticality of the assets. IT team provided sufficient information in terms of technologies that may have caused the assets vulnerable. As the last phase of the methodology suggests for developing a security strategy to protect the critical assets, a security strategic plan was developed and presented to the top management for review and approval. The OCTAVE methodology provided clear and transparent guidelines to evaluate vulnerable assets in the financial institution and helped to build a viable and useful security plan for the critical assets. The methodology was successfully implemented and Figure 1 shows the process

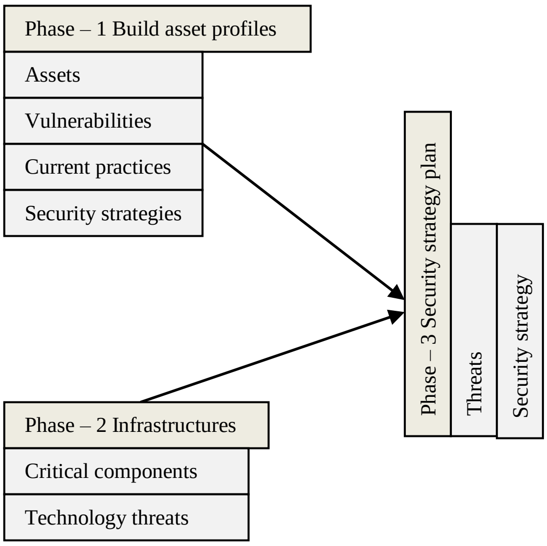

Figure. 1 Implemented OCTAVE methodology

4. RESULTS AND DISCUSSION

Since OCTAVE is a qualitative methodology a relative scale is used for determining probability of a risk to be occurred. Table II shows the scale used in determining the occurrence of risk in critical assets

Table II. Scale to determine risk probability

Probability	Description
Very high	Threat has occurred earlier and it is likely to occur in the present condition
High	Threat has occurred in the past and it is likely to occur
Normal	Threat may occur
Low	Threat occurred seldom in the past and most likely not to occur
Very low	Threat very unlikely to occur and may occur in unusual circumstance

When the staff members of the financial institution discussed different critical assets they were provided with the above scale to gauge risk in the assets. Table III shows the data obtained by the staff about the risk assets

Table 2II. Data about risk probability

Threat	Probability	Description
Hacker	Low	Intruder may access data or deny accessibility to data
Theft	Very low	A person/employee may steal data or devices physically
Data integrity	Very low	Information can be altered without authorization
Authorization	High	Accessibility to physical system without permission
Firewalls	Very low	Insufficient security to protect systems and data
Virus/worm	Low	Spread of malicious programs within organization
Disaster	Very low	An insider or outsider of the organization may destroy data
Cloud computing	Normal	Concerns of data security over cloud
Encryption	Very low	Encoded data captured and modified
Denial of service	Normal	Unavailability of service to legitimate customers or users

The above data clearly shows that assets in the financial institutions are somehow secure, although some threats need to be handled properly. For example, during discussion it was informed that sometime unauthorized personnel enter in operational areas for socializing with friends which may be threat for information assets. This methodology provided an opportunity to the management for making strict policy to ban entry to unauthorized people in operational areas. Similarly, latest technologies and updated versions of software are needed to secure the assets as at times service was unavailable to customers for some time and hackers blocked the traffic of data to pass through the servers of the institution. By this methodology the management was able to identify various vulnerable assets and obsolete technologies to be updated or replaced. At the end management was recommended a to prepare a detailed security strategy to protect the information assets.

In future, researchers may explore other type of organizations and threats and assess with different methodology. The methodology used in this study quite simple and easy to implement and can be used further in different type of organizations.

5. REFERENCES

[1] Jourdan, Z, Rainer, K., Marshall, E., and Ford, N. 2010 An investigation of organizational information security risk analysis. Journal of Service Science. 3, 33-42

[2] Syalim, A., Hori, Y., and Sakurai, K. 2009 Comparison of risk analysis methods: Microsoft' security management guide. International conference on availability, reliability and security. 726-731

[3] Saleh, S., and Alfantookh, A. 2011 A new comprehensive framework for enterprise information security risk management. Applied Computing and Informatics. 9, 107-118

[4] Palaniappan, S., Rabiah, A., and Mariana, Y. 2013 A conceptual framework of info structure for information security risk assessment. Journal of Information Security and Applications. 18, 45-52

[5] Ben, R., Jouini, M., Ben, A., and Milli, A. 2012 A cyber security model in cloud computing environments. Journal of King Saud University. 1, 63-75

[6] OCTAVE, http://www.cert.org/resilience/products-services/octave/index.cfm", [Retrieved on May 23, 2017]