IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A STUDY ON INFORMATION SECURITY AND RISK MANAGEMENT IN I.T. ORGANIZATIONS

K.Madhavan*, Dr.R.ManickaChezian

* Research scholar Research & DevelopmentCentre Bharathiar University Coimbatore - 641 046 Tamilnadu.

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

ABSTRACT

Information is the primary asset for any organization. The security to the information should be given utmost importance and reducing the risk of information compromise is a high priority.The importance that the organizations are paying towards information security risk has grown tremendously in the recent decades. A large number of risk assessment models have been proposed.The difference between these models lies in the different perspectives that each one focus on addressing the problems related to information security risk assessment. Some models are generic which can be applied to any organization, while others are specific, not suitable for all the risks in information security. The aim of the study is to make comparison between information security risk assessment models in terms of their activities, inputs and outputs required. The result of the study will have major implication for the organizations in helping them identifying a suitable model for information security risk assessment based on their specific requirements. The study is a part of a major research work aimed at developing an information security risk assessment method for I.T organizations based on using data mining technique.

KEYWORDS: risk analysis; risk assessment; risk analysis models; risk analysis method; risk analysis comparison; information security risk analysis method.

INTRODUCTION

Organizations around the world experience great difficultyin dealing with securing the information in a proper manner. Ensuring security to the informationassets is becoming a costly affair. In addition, new threats in the form of virus attacks are detected each and every day, which are capable of causing more undesirable consequences to the safety and security of information assets. Securing the IT infrastructure and IT assets is a difficult task and often expensive.In addition to the direct costs like planning, designing, and implementing safeguards, information security also requires the participation and cooperation of everyone in the organization but limits their freedom to use the technology to its fullest extent.

Organizations are operating in a globalized world where interoperabilitybetween the organizationsare significantly important. It is important that the security incidents should be taken care of properly and responses should be timely to maintain the interoperability nature of business. Thus, a need for systematic and planned efforts to deal with the information security challenge assumes significance.

INFORMATION SECURITY RISK MANAGEMENT

Information security is defined as the broad range of activities aimed in protection or preservation of four key aspects of information: availability, integrity, authenticity, and confidentiality.

- Availability: Approachability of information for different purposes.
- Integrity: Completeness, wholeness, and readability of information, and the quality of being unchanged from a baseline state.
- Authenticity: Validity, conformance, and genuineness of information.
- Confidentiality: Limited observation and disclosure of knowledge to only authorized individuals.

Risk management is becoming one of the most prevalent business issues in our days and manycompanies regard it as a critical but challenging endeavour. It's, however, a very broad concept thatembraces several types of risk.

INFORMATION SECURITY RISK ANALYSIS

Risk analysis generally involves the following tasks:

- ***Identification of* assets*:*** Information(databases and data files, contracts andagreements, system documentation, researchinformation, user manuals, training material,working *or* support procedures, businessendurance plans, fall back arrangements, audittrails, and archived information); SoftwareAssets (applicationsoftware,system software,development tools, and utilities); PhysicalAssets (computer equipment, communicationsequipment, removable media, and otherapparatus);Services(computing andcommunications services, general utilities, e.g.heating, lighting, power, and air-conditioning);People, and their qualifications, skills, andexperience; Intangibles, such as prominenceand image of the organization.
- **Identification of legal and business requirements** relevant for the identified assets.
- **Collecting all policies, procedures and controls** currently in place. Assess whether ornot the existing policies, procedures andcontrols implemented are satisfactory.
- **Identification of substantial threats or risk sources**. These threats can be fragmented intoHuman and Nonhuman elements. (Acts ofnature, acts of war, accidents, among othersmalicious acts originating from inside oroutside the organization).
- **Identification of vulnerabilities for the identified assets**.

Some of the common terms used in the information security risk management are given below:

- **Asset** can be defined as whatever having value to an organization.
- **Threat** is a latent cause of an unwanted incident, whichmay result in harming a system or organization.
- **Vulnerability** is a weakness of an asset/group ofassets that can be exploited by one or more threats. It isthe susceptibility to injury or attack. In computersecurity, the term vulnerability is applied to a weaknessin a system which allows an attacker to intrude upon theintegrity of that system.
- A **requirement** is a singular documented need of whata specific asset should be, do or respect.
- **Impact** is the severity of theconsequences of an event or incident. In the context of information security, the impact is a loss ofavailability, integrity, and confidentiality of information.
- **Likelihood** is the probability that the threat is likely to show up

RISK ANALYSIS METHODS

The purpose of any risk analysis is providing decision-makers with the best possible information about the probability of loss. As a result, it is important that decision-makers accept the risk analysis method used, and that information resulting from the analysis should be in a useful form. There are several different approaches to risk analysis, but they can be broken down into two essential types: quantitative and qualitative.

- Quantitative Risk Analysis

  This approach uses two basic elements: the probability of an event occurring and the losses that may be incurred. Quantitative risk analysis uses one number produced from these elements. This is called the Expected Annual Loss (ALE) or Estimated Annual Cost (EAC). This is calculated for an event by simply multiplying by the probability of potential losses. Therefore, in theory, one may rank events in order of risk (ALE) and make decisions based on that risk.
- Qualitative Risk Analysis

  The qualitative method rates the magnitude of the potential impact of a threat as high, medium, or low. Qualitative methods are the most common measures of the impact of risks. This method allows covered entities to assess all potential impacts, whether they are touchable or untouchable. The qualitative risk analysis methodology uses several elements such as threats, vulnerabilities and controls that are all interconnected.

Risk analysis includes processes such as the identification of activities, threat analysis, vulnerability analysis and guarantees. Risk analysis processes such as BS7799, GMIT, and CSE and explain the procedure to define the modalities for implementation. There are several methods used for analysis: a matched comparison of dependency diagrams, asset-function assignment tables, and activities. Other models for the design of information security focus on the identification and assessment of the vulnerability of the system and the specification of counters to those vulnerabilities.

RISK ASSESSMENT

Risk assessment is the process of identifying, characterizing, and understanding risk. It involves studying, analyzing, and describing the set of outcomes and likelihoods for a given endeavor. These methodologies centered on fault/event trees that were used to illustrate and to capture all possible plant failure modes in a graphical representation.

5.1 Quantitative and Qualitative Models of Risk Assessment

Riskassessment models can be broadly classified into quantitative and qualitative models.

5.1.1 Quantitative models

Quantitativemodels use measurable, objective data todetermine asset value, probability or loss, andaccompanying risk(s). The goal is to try tocalculate objective numeric values for each ofthe components gathered during the riskassessment and cost-benefit analysis.

Advantages

- Risks are prioritized by financial impact; assets are prioritized by financial values.
- Results facilitate management of risk by return on security investment.
- Results can be expressed in management-specific terminology (for example, monetaryvalues and probability expressed as a specific percentage).
- Accuracy tends to increase over time as the organization builds historic record of data while gaining experience.

Disadvantages

- Impact values assignedto risks are based onsubjective opinions ofparticipants.
- Process to reachcredible results andconsensus is very timeconsuming.
- Calculations can becomplex and timeconsuming.
- Results are presented inmonetary terms only,and they may bedifficult for nontechnicalpeople tointerpret.
- Process requiresexpertise, so participantscannot be easilycoached through it.

Qualitative Models

Qualitative methods use a relative measure ofrisk or asset value based on ranking orseparation into expressive categories such aslow, medium, high; not important, important,very important; or on a scale from 1 to 10. Aqualitative model evaluates the impact andlikelihood of the identified risks in a rapid andcost-effective manner. The sets of risksrecorded and analysed in qualitative riskassessment can provide a foundation for an attentive quantitative assessment. Bothqualitative and quantitative approaches tosecurity risk management have theiradvantages and disadvantages.

Advantages

Enables visibility andunderstanding of riskranking.

- Easier to reachconsensus
- Not necessary toquantify threatfrequency.
- Not necessary todeterminefinancial values ofassets.
- Easier to involvepeople who are notexperts on security orcomputers.

Disadvantages

- Insufficientdifferentiation betweenimportant risks.
- Difficult to justifyinvesting in controlimplementation becausethere is no basis for acost benefit analysis.
- Results are dependentupon the quality of therisk management teamthat is created.

Certainsituations may call for organizations toimplement the quantitative approach.Alternatively, organizations of small size orwith limited resources will probably find thequalitative approach much more to their liking.

Comparison of Information Security Risk Assessment Methods

In this section, information security assessment methods are presented, which have become best practices.

IT Grundschutz

The ‘IT Grundschutz’ or baseline protection manual (BSI, 2008), issued by the German ederal Office for Information Security (BSI - BundesamtfürSicherheit in der Informationstechnik). It provides a set of implementation guidelines, basic protection measures and guidance on system configuration. The baseline protection manual consists of standards, catalogues and tools to support information security. It also includes standards like BSI-Standard 100-1: Information Security Management Systems (ISMS), BSI Standard 100-2 IT-baseline protection methodology, BSI Standard 100-3: Risk Analysis based on baseline protection, BSI Standard 100-4: Business Continuity Management,
In the “IT Baseline Protection Manual” standard, security measures for typical business processes, applications and IT systems are proposed. The aim is to provide adequate protection for all of an institution’s information. The standard contains a brief description of the considered assets, procedures and IT systems, and an overview of security concerns and safeguards. Through the application of security measures for a system described in the standard, a proper security level can be achieved at the organisation.

Standard of Good Practice

The “Standard of Good Practice” for information security from the Information Security Forum (ISF) was designed to help any organisation - irrespective of market sector, size or structure - to keep the business risks associated with its information systems within acceptable limits (ISF, 2005). The standard covers five major areas: security management, critical business applications, computer installations, networks and system development. In each area, further subareas are defined, which are then subdivided into sections. For each section, the corresponding principles and objectives are set, all the while describing what needs to be done and why with regard to information security. According to the ISF, the standard can be used to improve the level of security in an organisation in a number of ways: by assessing the performance of information security, by supporting security audits/reviews, and by checking compliance. The ISF standard claims to be the international benchmark on information security.

CCTA Risk Analysis and Management Method (CRAMM)

CRAMM was developed by the British government organisation, CentralCommunication and Telecommunication Agency (CCTA), which has since beenrenamed the Office of Government Commerce (OGC) (CCTA, 1987). CRAMM hasthree stages: identifying the scope of review, assessing threats and vulnerabilitiesand proposing countermeasures for risk. In the first stage, physical assets aredetermined and valued by “what if” questions. Secondly, assets are grouped andthreat/vulnerability questionnaires performed. The responses to the questionnairesare scored and used to determine the level of risk. In stage three,countermeasures are proposed based on a list of safeguards. CRAMM provides aframework to calculate risks from asset values and vulnerabilities. The idea is thatthe potential damage of an event can be identified by the value of the asset. Theevent is assessed on the likelihood and impact based on the three categories:integrity, confidentiality and availability. The necessary data for the assessment iscollected via interviews.

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

OCTAVE (Alberts et al., 2003) was developed by the Carnegie Mellon Software EngineeringInstitute (SEI), is a framework to identify and manage information security risks.The assessment has three major phases: building security requirements,identifying infrastructure vulnerabilities and determining a security riskmanagement strategy. Assets and risks are identified with structured interviews.OCTAVE focuses on organizational risk and security practices rather than onspecific technology or system evaluations. In the first phase, the critical assets ofthe organisation are identified by business and IT personnel, along with the currentmeasures in place to protect these assets, security requirements and threats.Then, the related information technology components of the assets are identifiedand evaluated as to whether they are vulnerable to attacks. Finally, the risks to thecritical assets of the organisation are identified, whereafter strategies and plans formitigation are developed. OCTAVE uses security requirements to determine howan information asset is to be protected. Security requirements for confidentiality,integrity and availability are described verbally for critical assets and used forevaluation purposes.

OCTAVE Allegro

OCTAVE Allegro (Caralli et al., 2007) was developed by the Carnegie Mellon Software Engineering Institute (SEI), is a streamlined and fine-tuned version of the OCTAVE framework. OCTAVE framework was improved in terms of ease of use, resource requirements, risk results and compliance requirements. The goal of OCTAVE Allegro is to produce more robust results without extensive risk assessment knowledge and resource requirements. The focus of OCTAVE Allegro is on information assets and the context in which the information is used. OCTAVE Allegro consists of four phases and eight steps.

- Phase 1 - develop risk measurement criteria. Here, a qualitative set of measures has to be defined against the risks and evaluated.
- Phase 2 - create a profile for each critical information asset. The most important assets are noted, as well as technical containers, physical locations and people.
- Phase 3 - identify threats to each information asset. These areas of concern are then expanded into threat scenarios (situations where the information asset can be compromised).
- Phase 4 - identify and analyse risks to information assets and develop mitigation measures. The threat scenarios created in phase 4 are evaluated, and the consequences are determined and rated against the measurement criteria of phase 1. For risks that were evaluated as ‘high’, an appropriate mitigation approach is defined.

Control Objectives for Information and Related Technology (COBIT)
COBIT (ITGI, 2007) is a control framework for IT governance to link business goals with IT goals and the effective management of IT. The framework consists of 34 processes in four different domains, namely: plan and organise, acquire and implement, deliver and support, and monitor and evaluate. Within each domain, processes are defined with corresponding control objectives and controls, which can then be used to evaluate the current situation in an organisation. The adherence to these defined controls should provide assurance that business objectives will be achieved and undesired events will be detected, prevented or corrected. For each COBIT process, key goals and metrics are provided to measure the performance and outcome deviations. At the top right of the figure, the domain is shown (e.g. Plan and Organise). On the left, the process, requirements and control objectives and metrics are described for the process in a kind of waterfall. At the top left, the information criteria to be followed are defined. At the lower right, the IT resources for achieving the business requirement are indicated.

CORAS
The CORASrisk management process is mainly based on the risk management standard AS/NZS 4360 (ASNZ, 2004) and the information security standard ISO/EC 17799 (ISO, 2005c). CORAS has five main phases based on AS/NZS 4360: (1) identify context; (2) identify risks; (3) analyse risks; (4) evaluate risks; and (5) treat risks. Each is supported by models that should be constructed, as well as advice on how they should be expressed. At every phase, different methods of risk analysis are adapted, extended or combined - for example, Event-Tree-Analysis, Markov, HazOp and FMECA are all used. The platform uses open-source technologies like Java, XML and UML profiles for a model-based risk analysis of security-critical systems.

Information Security Management Maturity Model (ISM3)
The Information Security Management Maturity model (ISM3, 2007) is a framework for security management developed by an industry consortium. The framework describes common information security processes with underlying performance targets and metrics. The ISM3 handbook describes the security processes for each of the four categories - general, strategic management, tactical management and operational management - and the rationale behind choosing these processes. For each of those described, parameters such as output, input, activities and responsibilities are defined. These can be used to evaluate the current security maturity of the organisation and form the maturity level rating.

NIST Risk Management Guide SP 800-30
The National Institute of Standards and Technology (NIST) Risk Management Guide for Information Technology Systems Special Publication (SP) 800-30 (Stoneburner et al., 2002b) provides a foundation for developing an effective risk management programme. NIST was founded in 1901 by an agency of the U.S. Department of Commerce. Its goal is to promote competitiveness by advancing measurement science, standards and technology. The main focuses of NISTSP 800-30 are the risk assessment and risk mitigation processes. Therefore the guideline, through several steps, describes how to identify, determine, mitigate and document risks. For each process step, the inputs, outputs, and the activities to be performed are defined. The activities primarily describe the risk assessment procedure, suggesting how to perform these activities.

IT Infrastructure Library (ITIL)
The IT Infrastructure Library (ITIL) (CCTA, 2007) is a set of best practice processes and concepts published by the UK Office of Government and Commerce (OGC). The main focus of ITIL is on IT service management; it provides descriptions of processes to help implement and manage IT services. The two key building blocks of ITIL (version 2)

are service delivery and service support, the former of which is about the proactive management of the service provided - it contains sub-processes such as capacity management, availability management and continuity management. Service support, meanwhile, concentrates on the user and the support of business functions. Within service support, there are also sub-processes such as service desks, problem management, change management and configuration management. Another separate aspect of ITIL is security management, where the organizational involvement of information security is described. The content of this set of best practice processes is mainly based on the ISO 17799 (ISO, 2005c) standard, and describes how service support and delivery are affected by security management.

Expression of Needs and Identification of Security Objectives (EBIOS)

EBIOS (ANSSI, 2010b) was published in 1995 and developed by the DCSSI (Direction Centrale de la Sécurité des Systèmesd'Information), the French Ministry of Defense. The EBIOS method consists of a set of principles - analysis of the context, expression of security needs, threat study, identification of security objectives and security requirements. Firstly, the context has to be analysed with regard to general requirements, the owner of systems as well as further information about the assessment. Then, the security needs and the threats are identified in two separate activities. Security needs are expressed in terms of availability, integrity and confidentiality by the system users. Threats are identified by spotting attack methods and the corresponding vulnerabilities of the system. Within the next activity, “identification of security objectives”, risks are determined by combining threats and their impact on security needs. Security objectives of the system are evaluated with regard to the risk identified, and whether there are any conflicts between them. In the final activity, the necessary and sufficient security requirements are determined and the security controls contributing to the requirements are checked. Any residual risks are shown by comparing the security requirements and controls to the risks.

Harmonised Risk Analysis Method (MEHARI)

MEHARI (CLUSIF, 2010) is a risk assessment method developed by CLUSIF (Club for the Security of Information in France, or Club de la Sécurité de l'InformationFrançais).The MEHARI risk assessment is based on a knowledge base that has to be developed before the risk assessment. The knowledge base contains assets and potential damages to these assets (including vulnerabilities and threats), which form the basis for the risk scenarios (events or threats impacting upon an asset, with a rating of likeliness of any impact for the company). Based on the risk scenarios that were determined, the risks and their corresponding parameters are evaluated, bearing in mind the likelihood and impact of the risk.

Generally Accepted Information Security Principles (GAISP)

GAISP (ISSA, 2004) contains a set of security principles that were proven and accepted in practice. GAISPwas published by the Information Systems Security Association (ISSA) but was originally drafted by the Information Security Forum (ISF). Its principles are subdivided into pervasive, broad functional, and detailed. Pervasive principles provide general governance-level guidance to establish and maintain the security of information. The broad functional principles describe what to do at a high level of the pervasive principles, allowing a definition of the basic units of those principles. The detailed principles describe the methods of achieving the broad functional principles, with reference to the specific environment and current technology

Livermore Risk Analysis Methodology (LRAM)

The Livermore Risk Analysis Methodology (LRAM) was developed by Guarro et al. (1987) at the Lawrence Livermore National Laboratory. LRAMuses risk scenarios also called as “risk elements”. Firstly, in the information gathering phase, the data of systems are identified. Then risk scenarios are created containing the data systems, determining their monetary value, loss consequences, and possible threats. The evaluation of the risk scenario is conducted, both with no controls, and all controls applied, in order to determine the level of security. Various phases in LRAM consists of planning, risk analysis and management decision support. Each phaseends with the prioritisation and selection of the proposed control sets.

CONCLUSION

In the present security environment it becomes highly impracticableto provide complete protection to information systems inorganizations. Moreover, large number of methodologies are currently availablefor risk assessment. Organizations are facing the daunting task of choosing the right information security risk assessment method. The focus of the current study was analyzing the 14methodologies in detail and recognizing some common criteria. The analysis will help organizations in selecting the particular methodology in an easier and accurate manner. The important point is that the methodology chosen for risk assessment should meet all information security requirements and should fit into the existing corporate and IT domination configurations.

REFERENCES

[1] Guarro, S. (1987), 'Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management', *Computers & Security*, 6, pp. 493–504.

[2] ISSA (2004), *Generally Accepted Information Security Principles (GAISP)*, Information Systems Security Association (ISSA) [Online]. Available at https://www.issa.org/ (Accessed 15 November 2015).

[3] CLUSIF (2010), *Mehari 2010 - Risk assessment and treatment Guide*, CLUSIFClub de la Sécurité de l'InformationFrançais [Online]. Available at http://www.clusif.asso.fr/en/clusif/present/ (Accessed 10 November 2015).

[4] ANSSI (2010*b*), *Expression des Besoins et Identification des Objectifs de Sécurité - EBIOS - MÉTHODE DE GESTION DES RISQUES*, ANSSI - Agencenationale de la sécurité des systèmesd'information [Online]. Available at http://www.ssi.gouv.fr/en/the-anssi/, (Accessed 15 November 2015).

[5] ISO (2005*c*), *ISO 17799:2005 Information technology - Security techniques – Code of practice for information security management*, International Organization of Standardization (ISO).

[6] CCTA (2007), *IT Infrastructure Library (ITIL) Version 3*, Central Computing and Telecommunications Agency (CCTA).

[7] Stoneburner, G., Goguen, A. and Feringa, A. (2002*b*), *NIST Special Publication 800-30: Risk management guide for information technology systems*, National Institute of Standards and Technology (NIST) [Online]. Available at http://www.nist.gov (Accessed 10 November 2015).

[8] ISM3 (2007), *Information Security Management Maturity Model (ISM3)*, ISM3 Consortium [Online]. Available at http://www.ism3.com/ (Accessed 10 November 2015).

[9] Braber, Hogganvik, Lund, Stølen and Vraalsen (2007), 'Model-based security analysis in seven steps - a guided tour to the coras method', *BT Technology Journal* Vol. 25, No 1, pp. 101–117.

[10] ASNZ (2004), *Australian/New Zealand Standard Risk Management AS/NZS 4360:2004*, Australian and New Zealand Standards Committee.

[11] ISO (2005*c*), *ISO 17799:2005 Information technology - Security techniques – Code of practice for information security management*, International Organization of Standardization (ISO).

[12] ITGI (2007), *Control Objectives for Information and related Technology (COBIT), Version 4.1*, IT Governance Institute (ITGI) [Online]. Available at http://www.isaca.org/COBIT/Pages/default.aspx (Accessed 10 November 2015).

[13] Caralli, R., Stevens, J., Young, L. and Wilson, W. (2007), *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, Software Engineering Institute (SEI), Carnegie Mellon University, Pittsburgh, USA, CMU/SEI-2007-TR-012; ESC-TR-2007-012.

[14] Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003), *Introduction to the OCTAVE approach*, Software Engineering Institute (SEI), Carnegie Mellon University, Pittsburgh, USA, PA 15213-3890.

[15] CCTA (1987), *CCTA Risk Analysis and Management Method* [Online], Central Computing and Telecommunications Agency (CCTA). Available at http://www.cramm.com/ (Accessed 10 November 2015).

[16] ISF (2005), *The Standard of Good Practice for Information Security V4.1*, Information Security Forum (ISF) [Online]. Available at https://www.securityforum.org/ (Accessed 10 November 2015).

[17] BSI (2008), *BSI-Standard 100-02: IT-Grundschutz Methodology*, Federal Office of Information Security Germany (BSI).