Information Security and Risk Management for Banking System

Dr.Kodukula Subrahmanyam[1], M.Haritha[2,] V.Tejaswini[3], Ch.Balaram[4], C.Dheeraj[5].

4th year B.Tech Department of Computer Science and Engineering, K L University, Andhra Pradesh, India

***Abstract*:** *Risk management provides an effective approach for measuring the security, but existing risk management approaches come with major shortcomings such as the demand for a very detailed knowledge about the IT security sphere and the authentic company environment. Project risks are not always self-regulating, yet current risk management practices do not visibly manage the dependencies among risks. If dependencies can be clearly identified and analyzed, we can able to develop enhanced risk management strategies and make more effectual risk scheduling decisions. This paper proposes a management line of attack to address risk dependency issues. Through the study, we corroborate that risk dependencies do subsist in projects and can be identified and thoroughly managed. Risk and security management are very important issues in banking systems. Banking systems are complex with many entities, hazards and uncertainties. In such an atmosphere, it is very hard to initiate a system for evaluating and simulating the major hazards.*

Key *Words*: *Fuzzy logic, Information Security, Risk Management, Threat, Vulnerability.*

I. Introduction:

Major Aspects:

Confidentiality: Allowing only authoritative subjects admittance to information.

Integrity: Allowing only authorized subjects to change the information.

Availability: Ensuring that information and resources are handy when needed.

Nomenclature:

Risk: A risk is a potential event that will badly change the capability of a system to carry out its mission. A risk has two basic attributes- Probability P and Impact I. Probability stands for the possibility of the event occurrence. Impact refers to the consequences after the risk takes place. Risk Rx can thus be defined mathematically as a function of two attributes: Rx =f (Px, Ix).

Threat: Threat is the potential cause of an unwanted impact on a system or organization. Threat can also be defined as an undesired event (intentional or unintentional) that may cause damage to the merchandise of the organization.

Vulnerability: Vulnerability is a weakness or flaw in system actions, architectural system, its execution, internal control and other causes that can be subjugated to go around security systems and unofficial access to information.

Information security: Information security is the practice of defending information from unauthorized access, use, disclosure, disruption and modification.

II. Information Security:

Information security is now a foremost stream issue as the modern civilization is highly dependent on the use of Information Technology (IT) for commercial and confidential use. IT presents us with

a variety of risks like –physical risks and environmental risks, operational risks, safety risks, financial risks and, of course, information security risks. Security of new technologies / channels needs to be paid attention, for e.g., E-commerce, online banking and any other online transactions. This becomes still more essential in the radiance of increase in fraud associated losses in these areas along with the existing technologies and manual transaction processing risks.

All organizations today face a certain intensity of security risk. It is important to distinguish that all organizations agree to some level of risk. Risk is after all, a transaction between the amount of money you wish to spend on counter- measures, beside the perceived level of threat and vulnerability, to protect the predictable value of your assets. The important thing is that risk is identified, and either a) mitigated, b) transferred, c) insured, or d) clearly documented as a *risk acceptance*.

Banks have always been and are one of the most important targets for hackers, crackers and cyber criminals, as Information Security (IS) breach may lead to potential losses. Hence our aim is to identify the risks and handle them if the security is deployed. The actual losses on account of IS issues are not so easy to estimate.

III. Risk Management Process:

Risk management may be divided into three processes- Risk assessment, Risk mitigation, Effectiveness assessment. It should be distinguished that there is no universal conformity on these processes, but most views share the widespread elements of risk assessment and risk mitigation. Risk assessment is generally done to be aware of the system storing and processing the valuable information, system vulnerabilities, possible threats,

coercions, likely impact of the threats, and the risks posed to the system. Risk assessment would be purely a diligent exercise without the process of risk mitigation. Risk mitigation is a deliberate plan to prioritize the risks identified in risk assessment and take steps to selectively decrease the utmost priority risks under the constraints of an organization's partial possessions.

The third process is effectiveness assessment. The goal is to determine and confirm that the objectives of risk mitigation have been met. If not, the steps in risk assessment and risk mitigation may have to be rationalized. Essentially, effectiveness measurement gives feedback to the first two processes to ensure precision. Also, an organization's atmosphere is not permanent; hence there should be a frequent assessment process to update the risk mitigation tactic with new information.

Risk Assessment

It is unfeasible to know for what certain attacks will happen. Hence, risk depends on the probability of a threat. Also, a threat is not much of a risk if the confined system is not susceptible to that threat or, the potential loss is not significant. Risk is also a function of vulnerabilities and the expected impact of threats. Risk assessment involves a number of steps to understand the value of assets, system vulnerabilities, possible threats, threat likelihoods, and predictable impacts.

An overview of the process is

System characterization: It is obviously necessary to make out the information to protect its value and

the elements of the system (hardware, software, networks, processes, and people) that supports the storage, processing, and diffusion of information. This is often referred to as the information technology (IT) system. In other terms, the entire IT environment should be characterized in terms of resources, equipment, flow of information, and personnel responsibilities. System categorization can be done through some combination of personnel interviews, questionnaires, and reviews of documentation, on-site inspections, and automatic scanning.

Threat assessment: It is not possible to work out a defense approach without first understanding what to defend against. A threat is the potential for some damage or trouble to the IT environment. It is useful to make out the feasible causes or sources of threats. Although malicious attacks by human sources may come to mind first, the sources of threats are not unavoidably human. Sources can also be natural, for example, bad weather, floods, earthquakes, tornadoes, landslides, avalanches, etc. Sources can also be factors in the environment, such as power failures. Of course, human threats are on average the most troublesome because malicious attacks will be driven by intelligence and strategy. Not all human threats have a malicious intention; for example, a threat might come up from negligence such as forgetting to change a default computer account or accident, possibly misconfiguring a firewall to allow unwanted traffic, or unwittingly downloading malicious software.

Vulnerability analysis: Threats should be viewed in the circumstance of vulnerabilities. Vulnerability is a weakness that might be exploited. A threat is not virtually important if the system is not susceptible to that threat. It is common practice to use automated vulnerability scanning tools to evaluate an operational system. Several free and commercial vulnerability scanners are available such as Satan, Sara, Saint, and Nesses. These scanners basically contain a catalog of known vulnerabilities and test a system for these vulnerabilities by snooping. Another method to find out vulnerabilities in a system is penetration testing which simulates the actions of an attacker. The assumption is that active attacks will help to reveal weaknesses in system defenses. Not all vulnerabilities are necessarily technical and well defined. Vulnerabilities might come up from security management and system operations. Security policies may be partial, exposing the system to possible negotiation.

IV. Risk Mitigation:

The process of risk mitigation is to deliberately invest limited resources to change intolerable risks into tolerable ones. Risk mitigation may be a combination of technological and nontechnical changes. Technological changes involve security equipment (e.g., access controls, cryptography, firewalls, intrusion detection systems, physical security, antivirus software, audit trails, backups) and management of that equipment. Non-technical changes could include policy changes, user training, and security awareness. An outline of the steps in risk mitigation is described below.

Prioritize actions: The risks with their consequent levels identified through the risk assessment process will recommend what actions should be taken. Obviously, the risks with unacceptably high levels should be addressed with the greatest urgency. This step should make out a ranked list of actions required to address the well-known risks.

Identify possible controls: This step examines all the prone actions to mitigate risks. Some controls will be more practical or cost effective than others, but that determination is left for later. The result from this step is a list of control options for advance study.

Select controls for implementation: The cost-benefit analysis from the preceding step is used to fix on which controls to implement measures to meet the organization's goals. Most probably, the recommended controls will require a budget, and the budget must be balanced against the organization's other budget demands. That is, the final assortment of controls to implement depends not only on the action priorities but also on all challenging priorities of the organization.

Assign responsibilities: Ultimately, implementation will depend on personnel i.e., human resources with the appropriate skills. The personnel might be available within an organization, but for any number of reasons, an organization might come to a decision to hand over responsibilities to a third party.

Implementation: In the final step, the selected controls must be implemented by the liable personnel.

V. Effectiveness Evaluation:

Effectiveness assessment is the process of measuring and verifying that the objectives of risk mitigation have been met. While risk assessment and risk mitigation are done at certain distinct times, the process of effectiveness evaluation must be continuously ongoing. As mentioned earlier, there are two realistic reasons for this process in risk management.

First, risk assessment is not an accurate discipline. There are uncertainties related to the real range of threats, likelihood of threats, impacts, and expected frequency. Similarly, in the risk mitigation process, there are uncertainties in the estimation of overheads and benefits for each control option. The uncertainties may result in misjudgments in the risk mitigation plan. Hence, an assessment of the success or failure of the risk mitigation plan is essential. It provides useful feedback into the process to guarantee the correctness.

Second, an organization's environment cannot be projected to remain static. In the fullness of time, an organization's network, computers, software, personnel, policies, and priorities will all change. Risk assessment and risk mitigation should be repeated or updated periodically to keep current.

We researched several alternative modeling techniques, such as the probabilistic theory, PERT (Program Evaluation and Review Technique) analysis, heuristic modeling, and fuzzy logic. We concluded that fuzzy-logic techniques present a plausible way of modeling such elusiveness, and we can relate the whole thing back to a certain degree of likelihood—for example, the chance that the user information will be exposed to outsiders might fall under the "high likelihood" fuzzy set, at a 68% chance. When users visit the bank website they can follow various routes, depending on the purpose of their visit and can proceed in further. Each user route consists of a finite number of phases. A *phase* is a division within a specified user route. It consists of phases like: registration, login, Online shopping, online transaction, statements, loan requests and balance enquiry visits. A typical user spends a certain amount of time in each phase of the route. During

each phase, the user information is basically shared by authorized communicating parties, such as the management.

VI. Dependency Analysis models:

Current project management practices do not plainly concentrate on how dependencies between risks are managed. In this section, we evaluate several dependency analysis models that have been used to represent the dependency of one event on another. There are three common tree-based analysis techniques.

First, fault tree is a logical diagram used in the Fault Tree Analysis (FTA) to represent the possible causes of an undesired occurrence/event. The root of the tree represents the undesired event, and the other events that lead to the root are modeled by independent leaf nodes with a series of logical expressions. For example, a fault tree can present the relation between the failure of a system and failures of the system components. Second, Event Tree Analysis is a method to illustrate the chain of possible outcomes after the occurrence of an undesired event. Similarly to a fault tree, an event tree starts from an undesired event, and the event is linked to its outcomes toward the final consequences with the likelihood of occurrence assigned to each tree branch. Last, cause-consequence analysis (CCA) combines the FTA and ETA and is performed with a cause consequence diagram which starts from an undesired event and develops backward to identify its causes (presented by a fault tree) and forward to make out its consequences (presented by an event tree). CCA can help to identify the chain of events from the initiators of an undesired event to its concluding consequences. Markov analysis provides a mathematical method to analyze the trustworthiness and ease of use of systems which are well precise and have strong component dependencies. In this analysis, a system is modeled as a number of discrete states with likely transitions among the states. The states are graphically presented as nodes in a directed graph, where the edges correspond to the probabilities of going from one node to another node. In accordance with the probability distribution, the system transits from its current state to the next state. In a Bayesian network, each node represents a variable and each arc represents causal or probabilistic influential relationships between variables. A link between two variables represents a probabilistic dependency between them. When a Bayesian network is analyzed qualitatively, it provides the relations of causes and effects between nodes. If a Bayesian network is analyzed quantitatively, it is a representation of a joint probability distribution in which each node is associated with a conditional probability distribution reflecting its parent nodes. When the links are interpreted as direct causal influences between variables, the network is called a Causal Network. Bayesian network is often used, particularly when it is applied with probability theory, to handle uncertainty by plainly presenting the conditional dependencies between different knowledge workings. However, the computations involving a reasonable number of variables are often composite and the assistance of appropriate tools is required. A goal model, represented as a directed graph, is used to refine the goals of a target system by disintegration into measurable sub goals. Tropos goal model is a goal model framework like structure for requirement analysis by refining stakeholders' goals. This structure allows analysts to model the influence of

the fulfillment of a goal to the satisfaction of other goals. The Goal-Risk Model is a risk modeling and reasoning framework that further extends the Tropos goal model into three layers: Goal, Event, and Treatment. The analysis starts by identifying an appropriate event that can influence any goals in the goal layer. The event is decomposed with contribution associations until all of its leaf events are mutually restricted. Once the events have been analyzed, corresponding treatments are identified and analyzed.

VII. Figures:

Figure 1

VIII. Conclusion:

Information security is an enduring process to handle risks. One could say that risk management is basically a decision making process. The risk assessment stage is the assortment of information that is input into the decision. The risk mitigation stage is the actual decision making and implementation of the resultant approach. The effectiveness assessment is the continual feedback into the decision making.

This Cognitive Fuzzy Approach is unique because it uses both the FCM and the fuzzy-rule-based techniques to compute the IT risk value linked to a phase in an explicit user route. The advantage of using these techniques together is that it takes into account intuitive user transactions, which forms the basis of any risk assessment, and also accounts for the ambiguity regarding user information and risks when calculating a phase's risk level in a typical user route. By identifying a phase's IT risk value, this approach helps bank staff manage risks by facilitating the decision-making process.

IX. Acknowledgement

I express my sincere gratitude Dr. K. Subrahmanyam from K L University, Green Fields, Vaddeswaram for his guidance and support. This time I remember my parents with great reverence whose support and prayers are always my strength. I would also like to thank my friends for their support.

References:

1. Alberts C and Dorofee, A. (2002) Managing information security risks: the OCTAVE approach. Reading, MA: Addison Wesley.

2. B. Kosko, Fuzzy Engineering, Prentice Hall, Upper Saddle River, N.J., 1997, p. 549.

3. Gordon, L. A. and M. P. Loeb. 2001. A Framework for Using Information Security as a Response to Competitor Analysis Systems. Communications of the ACM 44, No, 9 (September): 70-75.

4. Peltier, T. (2005). *Information Security Risk Analysis*, 2nd ed. New York, NY: Auerbach Publications.

5. http://www.slideshare.net/m9821735 856/information-security-and-risk-management-for-banks

6. http://globaljournals.org/GJCST_Vol ume10/7-Information-Security-Risk-Assessment-for-Banking-Sector-A-Case-study-of-Pakistani-Banks.pdf