International Research Journal of Mathematics, Engineering and IT
ISSN: (2348-9766)
Association of Academic Researchers and Faculties (AARF)
Impact Factor- 5.489 Volume 7, Issue 2, February 2020
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

EMERGING TRENDS IN INFORMATION SECURITY RISK MANAGEMENT : A TRADITIONAL OVERVIEW

Devarshi Chatterjee[1] and Prof (Dr) Devapriya Chatterjee[2]

[1-] Student Member-CSI and Final Year Student of CSCE, KIIT University, Bhubaneswar, 751024, India,
[2-] Senior Member-CSI and Chartered Engineer (India), BB 73, Sector 1, Salt Lake City, Kolkata-700064, India,

Abstract

Information Security Risk Management involves more of traditional risk analysis and risk assessment. There are limitations of traditional tools in fundamental ways, such as lack of reliable frequency data about past risk events and the relative rarity of many kinds of risks that need to be managed. Information Security RiskManagement involves four types of risk treatments, like self-protection, risk transfer, self-insurance and risk avoidance. The paper introduces an approach to risk management in which risks and risk treatments are strategically managed using a portfolio approach. When there is a portfolio approach, different risk portfolios are managed through a portfolio of risk treatments. The limitations include lack of accuracy in predicting probabilities and losses from recognized threats.

Key Words : Security, Insurance, Analysis, Assessment, and Treatment

1. INTRODUCTION

Risk-analysis provides the basic cost-benefit justification for the acquisition of security safeguards, and is a well-established technique with proven past records. Information Security Risk Management is a central technique used in managing information system risks.The best characteristic of this technique is the ability to communicate to general management, the expert opinions about an organization's information risk profile in terms of threats and safeguards. We

find two intractable problems that limit the effectiveness of common risk analysis practices : a) lacking of reliable empirical data about the frequency and amount of losses attributable to Information Security compromises, and b) common relative rarity of many kinds of Information Security compromises. Utilization of risk analysis techniques requires compound calculations on a fairly large database of threats, frequency data and loss data.

2. HYPOTHESIS

The research contemplates four basic types of treatments for risk management. These are :

a) Self-protection : This type prevents risks from having an impact on the organization. In this category, the safeguards employed, are preventive in nature. Innovative technologies of the present era, like intrusion detection, firewalls, virus protection and software, etc represent the implementation of risk treatments in thisarea.

b) Risk Transfer : This type involves distributing all or part of the impact of certain risks across multiple organizations. In this category, mechanisms include the purchase ofthe insurance on the market,and the use of outsourcing to transfer parts of the risky information systems to otherorganizations.

c) Self-Insurance : This type involves various active forms of preparedness, like maintenance of savings accounts to provide funds necessary to restore normaloperations or maintaining excess capacity in information processing to permit the system to operate effectively when compromised and loaded with unauthorizedprocessing.

d) Avoidance : This type chooses to avoid going to businesses in the areas of threat of compromise, resulting in frequent high losses. The attacks of intrusion on consumer websites are frequent and the losses that follow the disclosure of banking information can be very high. Hence it is necessary to avoid processing or retaining customer carddata.

3. MATERIALS ANDMETHODS

The need for Information Security standards is not always eliminated by the use of a risk treatment framework, within the organization. These standards may be legislated by the government. The

Payment Card Industry Data Security Standard is an example of industry guideline. The quantitative Information Security Risk Management focuses on factual and measurable data and use mathematical formulae to determine the exposure factor and SLE

(Single Loss Expectancy-money expected to be lost if the incident occurs once), as well as the probability of a threat being realized, called the ARO (Annual Rate of Occurrence—how many times in a year the incident is expected to occur). The ALE (Annualized Loss Expectancy— money expected to be lost in one year, given by the product of SLE and ARO) is the risk value. The drawback is that there is no sufficient data to be analyzed, or the number of variables involved is very high, making analysis impractical. The qualitative Information Security Risk Management focuses on experience, judgment, and the probability of a risk occurring, with its
impact on relevant organizational aspects. The risk's final value is represented in scales as 'low-medium-high'. The drawback is that results are usually less precise.

4. RESULTS ANDDISCUSSION

The risk treatment framework, as given in Table 1, may be used for organizing the basic risk and risk treatment portfolio. The framework, together with the appropriate use of risk analysis and security standards, provide the basis on which Information Security managers can formulate sound risk strategies, that include the most appropriate treatments for the various Information Security threats the organization confronts. A portfolio arranges the different kinds of Information Security risks, faced by the organization, and organizes an appropriate collection of treatments that balance the portfolio. We have identified five best practices, as a process for developing the risk treatment portfolio, as given in Table 1. These are given by :

a) The definition of an overall organizational risk management strategy : This can be constructed from the risk treatment framework and used to incorporate processesfor identifying risks in developing risktreatments.

Table 1 :

The Layout of Risk and Treatment Portfolio

Category Portfolio	Risks Portfolio	Treatments Portfolio
Low impact, low frequency	Risk One	Treatment One Self-insurance
	Risk Two	Treatment Two Self-insurance
	Risk Three	Treatment Three Self-Insurance
High impact,low frequency	Risk One	Treatment One Risk Transfer
	Risk Two	Treatment Two Risk Transfer
	Risk Three	Treatment Three Risk Transfer
Low impact, high frequency	Risk One	Treatment One Self-Protection
	Risk Two	Treatment Two Self-Protection
	Risk Three	Treatment Three Self-Protection
High impact, high frequency	Risk One	Treatment One Avoidance
	Risk Two	Treatment Two Avoidance
	Risk Three	Treatment Three Avoidance

b) The adherence to the most useful IT security standard : The standard and risk analysis become a dialectic in which safeguards and controls are adopted as a result of the interplay and the tension between the universal inventory of controls and the economic justification of each control through risk analysis and cost benefit operation.

c) The development and deployment of safeguards and controls providing the optimal combination of risk treatments : These comprise of safeguards that collectively provide both preventive and recovery measures.

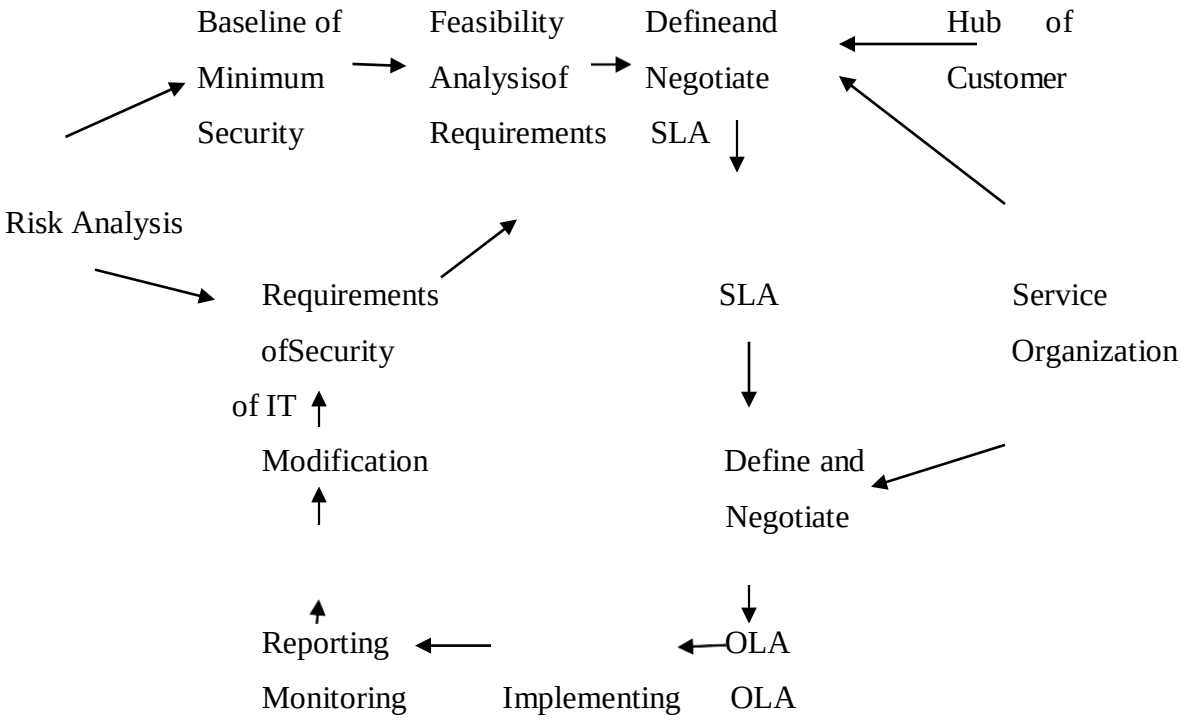
d) The providing of system risk review mechanisms : The mechanisms need to be formulated such that decisions can be made to cancel development of risky systems or risky parts of systems or opt out of risky information system components.

e) The testing of all risk treatments : These mechanisms need to include penetration testing.

The overall risk management framework is provided by these five practices, within which risk analysis plays an appropriate function. Risk analysis, here, is not the primary means for determining the appropriate safeguards, but a tool for fine tuning the decisions about individual treatments, appropriate for the categories of risks and treatments. The concepts of basic Information Security Risk Management are inadequate as a stand-alone approach to IT risk management, although several existing methodologies of Information Security adopt a similar approach. Whenever there is a strategic orientation of these methodologies, their adoption is made easier. The IT Infrastructural Library Security Management Process is developed with the best practices as a guide, and takes the focus of business strategy, with an orientation towards IT service delivery. This process develops four kinds of products, namely, policies, processes, procedures and work instructions. As a result, there is strategic correspondence to processes at the tactical and operational level. Figure 1 illustrates the method for developing these products, procedures and work instructions.

Figure 1

The Process of IT Infrastructure Library Security Management



5. FINDINGS AND CONTRIBUTION

Extensive research is needed to provide inventories of existing and new safeguards, both technical and managerial, that meet the different risk treatment categories. Such inventories will make the job of constructing risk management portfolios much more simple. The possible future research areas may be identified from Table 2.No inventory of security safeguards or controls are available, that are categorized by the risk treatment type. It needs to be decided by an IT Risk Manager, which control fits within each risk category, and then determine whether or not each control should be included in a particular portfolio. Managers may discover new kinds of safeguards or controls by thoughtful search of the solution space for different categories of risk treatments.

Table 2

Scope of Future Research

Area	Issue	Impact
1.Safeguards and controls ofsecurity	1.1 No published inventories of security safeguards or controls classified by risk treatmenttype 1.2 No clearinghouse for new kinds of safeguards andcontrols	Every designer must innovate control that fits each category Diffusion of security controls and safeguards is inhibited
2.Risk controls and safeguards success	2.1 Fit between safeguards and risk settings	We do not know what organizational characteristics best define ideal settings for certain risk treatments
3.Categories of treatments explored Improperly/poorly	3.1 What are the strategies for self-insurance?	Self-insurance needs to be elevated from 'no-doing' assumptions

a) Features on Table 2, Issue2.1

Further study is necessary to determine the fit between the risk treatment inventories and the organization. The general relationships between organization characteristics need better understanding to help risk management strategists to be more effective in selecting risk management portfolios.

b) Features on Table 2, Issue3.1

We need to study the different ways in which organizations can reduce the financial impact of a risk occurrence, apart from depositing reserve money into a savings account. An in-depth study is needed to expand our understanding of this category, and to explore and innovate new safeguards that enact this category of risk treatment for future strategic IT risk management portfolios.

6. CONCLUSION

We have explored the ways in which IT risk management can move beyond the direct activities of risk analysis or risk assessment. These traditional risk management tools are limited in fundamental ways, making them difficult in practice. While researching risk analysis, we establish that operational risk management involves four types of risk treatments : a) self- protection, b) risk transfer, c) self-insurance, and d) risk avoidance. It is concluded that a portfolio approach manages different risk portfolios with a matching portfolio of risk treatments.

7. REFERENCE

1. http://www.verizonenterprise.com/verizon-insights-lab/dbir
2. http://economictimes.indiatimes.com/news/economy/policy/india-needs-forensic-it-audits-for-banks-to-prevent-card-fraud/articleshow/55002400.cms
3. www.wikipedia.com
4. http://timesofindia.indiatimes.com/city/hyderabad/cyber-crime-cases-shoot-up-post-demonetization/articleshow/56129277.cms
5. http://www.hindustantimes.com/delhi/man-fined-for-posting-ex-girlfriend-s-photo/story-I9KGe1mHV6wzr3sAJdk8BK.html