Volume 2, Issue 12, December 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Study of Risk Management of an Information System by Assessing Threat, Vulnerability and Countermeasure

Venkata Kiran Maram*
Dept of Computer Applications
CMJ University
Bangalore, India

Dr. Mohammad Sharif K B
Dept of Computer Applications
CRD Business School
Bangalore, India

Badri H.S
Dept of Computer Applications
Presidency College
Bangalore, India

Abstract: ***Countermeasure is a way to plan ahead to secure an information system. However, it cannot be assured total protection against all threats. An essential part of any risk management plan is to evaluate system threats and vulnerability facing the system. Threats are intended to/or have the capability to accomplish their intentions. These types of threat and measures that may be taken to reduce or eliminate the risks they create are the principal subject of this paper. Using a numerical experiment, this paper models a mock-up of how countermeasures correspond with the level of risk.***

Keywords: Countermeasure, Vulnerability, Risk Assessment, Threat, Information System Security, Security Policy.

I. INTRODUCTION

Information security is the protection of information from threats and ensures business continuity by minimizing business risk, and maximizing return on investments and business opportunities. [7] Information systems are generally defined by an organization's assets that allow a company cares the organization's business. This is especially important in the increasingly interconnected business environment. As information systems are vital to organization it must be protected. In this case, information system security generally consists in ensuring that an organization's material and software resources are used only for their intended purposes. [2, 6]. The security attention in information systems has grown in recent years according to their diffusion, the increasing role they have in contexts in which they operate and their increasing complexity and exposure to possible attacks. [1, 2, 3] In strategic terms, it must be emphasized alongside the availability and integrity of information, often crucial to ensure continuity. According to the International Organization for Standardization (ISO) definition, security is the set of measures to ensure the availability, integrity and confidentiality of information. It is essential for organizations to plan ahead against security breaches. To follow this course, contractor may offer a range of technical protection or firewall encryption. However, it is important to realize that the use of these techniques or other security requires careful and systematic planning. This leads to be able to implementation an optimal and appropriate controls within the organization.

It is important not to assume that countermeasures in an information system are not sufficient to prevent any attacks. To ensure a system, potential threats must be identified so as to identify and anticipate the enemy's course of action. [6] The system must prevent the direct or indirect alteration of the information, both by unauthorized users and processes, and as a result of accidental or negligence. The system must prevent any person from obtaining, directly or indirectly, information that is not authorized to access. Using a numerical experiment, in this paper a model is being created which mock-up how the countermeasure correspond with the level of risk. As countermeasure is any action taken to prevent the threat, risk management describe the threat environment in which the system works and the possible vulnerabilities which may occur. Threats correspond to the type of exploit that could be damage, whereas the vulnerability is the level of exposure to threats in a particular context. [3, 12]. A primary benefit of an effective countermeasure plan is to enable the organization to properly identify the appropriate level of resources and capabilities required to alleviate an attack. In response to an attack, an organization has to deploy resources and capabilities to repel it as quickly as possible. That purely reactive approach is extremely inefficient and can have significant financial consequences. [2, 3] A sound countermeasure plan can prevent expensive overreaction.

II. BACKGROUND: SECURITY ISSUES

In general, the objective of information security is to protect organizational activities to ensure business continuity, minimize business damage and maximize return on investment (as defined by ISO 17799). Information security is characterized by the preservation of: This practice focuses on areas commonly accepted in the community of information security: risk management, confidentiality, integrity and availability protection / response intrusion detection, identification and authentication, access control, administration of forest safety security. Information security management involves a mixture of anticipation, detection and response processes. It is also a series of actions and processes that require constant monitoring and control. [5] These series includes:

o Assessing security risk: performing security risk assessment to identify threats, vulnerabilities and impacts

o Implementing & maintaining a secure framework: defining and developing policies, assigning responsibilities and applying safeguard measures
o Monitoring & recording: monitoring and recording constantly so that proper arrangements can be made when tackling a security incident
o Reviewing & improving: conducting periodic review and security audit to make sure that adequate security controls are meeting security requirements

Security measures and countermeasures are intended to defend organizations from different security breaches. To plan security requirements of an organization, it is necessary to evaluate the current security needs of the organization as well as the measures to be taken to achieve such requirements. [10] This is done by categorizing information security level. [10, 11] As vulnerability of information systems can lead to attacks [10], assessing it can help identifying the flaws and weaknesses that could possibly be exploited of the threats. [4] The risk of vulnerability raises the threats which can take advantage of vulnerabilities to cause damage or loss. [9, 12] A security threat is a condition of vulnerability that may lead to an information security being compromised. [8] Security countermeasure refers to a method to expose, stop ,or reduce losses associated with a specific IS threat. [8, 11] Threats are often classify according to the type of assets concerned. Loch et al. [13] shaped a threat model that had four dimensions: sources, perpetrators, intent, and consequence, with threats occurring from the inside or outside with the perpetrators either be human or non-human and the actions accidental or intentional with the consequence a disclosure, modification, destruction, or denial of service [11] White et al. [14] in their study of responses to threats distinguished between internal and external IS security functions, where internal functions focused on technical issues, whereas external functions stressed managerial and operating security, or nontechnical issues. [13, 14] National Information Assurance [CNSS] describe operative IS security to protect as "information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats." [11].

III. COUNTERMEASURE, VULNERABILITY AN THREAT

A risk is derived from the analysis of a threat and vulnerability. Risk assessment involves determining relativity among risks and calculating associated damage or loss. This depends on the basis for effective countermeasures [8]. On the other hand a threat means any agent that could reduce or attempts to disable the efficiency of a system, thereby preventing or negating the functionality of the system. Here the word "threat" is used to describe component of risk, while vulnerabilities are characteristics that can be exploited by a threat. A vulnerability for which there is no credible threat does not require a response by the security processes. Careful attention to the design countermeasures can positively reduce or eliminate vulnerabilities [8, 12]. Where vulnerabilities are inherent or cost too much to eliminate during the design and development of facilities or systems, countermeasures must be selected to reduce risk to an acceptable level. Countermeasures may abate the danger even if there is both a malevolent and capable threat as well as a vulnerability which can be exploited by that threat.

No countermeasure is completely effective, and, short of complete destruction, the impact of damage to an asset is problematic. Risk management requires the realistic assessment of uncertainties. In practice, the estimations needed in applying a risk management process are accomplished in only gross terms. Threat level or uncertainty may be assessed as high or low. This gross quantification of factors in the risk management equation allows the design attributes used to reduce vulnerabilities and the countermeasures to be grouped so that they can be applied consistently. Knowing we cannot completely eliminate risk, this process permits us to manage the nature and amount of risk to achieve levels we can accept at costs we can afford.

No system is without vulnerability and no countermeasure is completely effective. Risk management requires a realistic assessment of uncertainties. Some inherent vulnerability cannot be fully eliminated, nor would the cost of the risk. In most cases, though, it is possible to balance the level of risk against the costs of countermeasures by selecting a combination of adequate. We can provide a reasonable, cost effective, and enduring framework using risk management as the underlying basis for securing the system.

Despite attempting to eliminate risk, it is impossible to eliminate. Even if we try to eliminate all risk, the price of attaining such goal comes extremely high. The results of such an analysis could include pragmatic decisions as to whether achieving risk avoidance at such cost is reasonable. Applying reason in choosing how much risk we can accept and, hence, how much security we can afford is risk management.

Security measures and countermeasures are meant to defend organizations from different security breaches. To plan security requirements of an organization, it is necessary to be able to evaluate the current security demands of an organization as well as the measures taken to achieve such requirements [10]. The purpose of applying security measures is to protect information security objectives and information assets. Information security objectives are the main concern in categorizing information security level [10, 11].

Vulnerability of information systems which can lead to attacks [10]. An attack on information systems is a sign of vulnerability. According to Dhillon vulnerability assessment deals with identifying flaws and weaknesses that could possibly be exploited of the threats. [10, 14] The risk of vulnerability raises the threats which can take advantage of vulnerabilities to cause damage or loss [9].

Threat is an indication of impending danger or harm [10, 16]. "A security threat is a condition of vulnerability that may lead to an information security being compromised." [8, 10].

IV. CONCLUSION

In this paper a model of how countermeasures correspond with the level of vulnerability and threat is presented. A vital element of any risk management plan is to assess level of threat and vulnerability a system may face. Threats are projected to harm or incapacitate a system. These types of threats and measures may reduce or eliminate the risks. Despite, increasing countermeasure lowers dramatically the level of risk, it can be said that it will be a waste of resource by topping up more resources. When threat is measured we have the level of risk to be measure. There must be some tolerable risk as it is almost impossible to have zero risk.

The following section outlines the C2 style for describing software architectures and presents the Elevator case study.
.

ACKNOWLEDGMENT

I am indebted to Dr. Mohammad Sharif Bammanalli for his valuable insights and guidance.

REFERENCES

[1] Leonforte, Antonio, La Sicurezza nei Sistemi Informativi, 2009.
http://www.villaumbra.org/resources/Documenti/Regio ne/sicurezza%20S.I.pdf, accessed on 29/02/2010.
[2] Siponen, Mikko, Designing secure information systems and software: Critical evaluation of the existing approaches and a new paradigm, 2007.
http://herkules.oulu.fi/isbn9514267907/html/ accessed
12/01/2010.
[3] Siponen, M.; Pahnila, S.; Mahmood, M.A.; , "Compliance with Information Security Policies: An Empirical Investigation," Computer , vol.43, no.2, pp.64-71, Feb. 2010 [4] Dhillon G, Managing SIS. MacMillan Press LTD, London, UK, 1997.
[5] InfoSec, Acceptable Use Policy,http://csc.colstate.edu/summers/e-library/policy.html, 2006, accessed on 10/042010.
[6] Kioskea, IT Security - Introduction to IT Security, http://en.kioskea.net/contents/secu/secuintro.php3, accessed on 15/03/2010.
[7] ISO/IEC 17799:2005, Information technology - Security
techniques - Code of practice for information security management,
http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm
, 2005, accessed on 12/04/2010.
[8] Kumar, R. L., Park, S., and Subramaniam, C.: Understanding the value of countermeasures portfolios in information systems security. Journal on Management Information Systems, 25, 241-279, 2008.
[9] Nyanchama, M.: Enterprise vulnerability management and its role in information security management. Information Systems Security, 14, 29-56, 2005.
[10] Abdullah Alshboul, Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks, IBIMA Publishing Communications of the IBIMA,
http://www.ibimapublishing.com/journals/CIBIMA/cib
ima.html, Vol. 2010, 2010
[11] Chen, C. C., Shaw, R. S., and Yang, S.C.: Mitigating information security risks by increasing user awareness: A case study of information security awareness system. Information Technology, Learning & Performance Journal, 24, 1-14, 2006.
[12] Daniel J. Ryan and Julie J. C. H. Ryan, Risk Management and Information Security, Computer Security Applications Conference, New Orleans, Louisiana, December 19, 1995 [13] K.D. Loch, H.H. Carr and M.E. Warkentin, Threats to information systems: today's reality, yesterday's understanding, MIS Quarterly 16 (2) (1992), pp. 173– 186
[14] G.B. White, E.A. Fisch and U.W. Pooch, Computer System and Network Security, CRC Press, Boca Raton, FL (1996).
[15] Dhillon, G. (2006). Principles of information systems security: Texts and Cases (1st ed.). Hoboken, NJ: Wiley. [16] Johnson, M. E. (2008). Information risk of inadvertent disclosure: An Analysis of File sharing risk in the financial chain. Journal of Management Information Systems, 25(2), 97-123.
[17] Mustaquim, M., Security Concern Throughout System Development Life Cycle,
http://www.groundreport.com/Media_and_Tech/Security- Concern-Throughout-System-Development-
Lif_18/2846835, 2007, accessed on 27/03/2010.

© 2012, IJARCSSE All Rights Reserved