INFORMATION SYSTEM AND RISK MANAGMANT STRATEGIES

Tinatin Mshvidobadze
Gori Teaching University, Georgia

Summary

This paper defines the understanding of risk. The risk-assessment methodology is essential in building an effectively and secure computing environment. Unfortunately, this is still a challenging area for information professionals due to the rate of change in technology, the relatively recent advent and explosive growth of the Internet, and perhaps the prevalence of the attitude (or reality) that assessing risk and identifying return on investment is simply too hard to do. On this background risk-assessment is very important. In the represented paper there are described the main threats and are given risk-management strategies.

Keywords: understanding of risk. quantitative. vulnerabilities and Defining likelihood.

1. Introduction

The fundamental precept of information security is to support the mission of the organization. All organizations are exposed to uncertainties, some of which impact the organization in a negative manner. In order to support the organization, IT security professionals must be able to help their organizations' management understand and manage these uncertainties.

Managing uncertainties is not an easy task. Limited resources and an ever-changing landscape of threats and vulnerabilities make completely mitigating all risks impossible. Therefore, IT security professionals must have a toolset to assist them in sharing a commonly understood view with IT and business managers concerning the potential impact of various IT security related threats to the mission. This toolset needs to be consistent, repeatable, cost-effective and reduce risks to a reasonable level.

Risk is the potential harm that may arise from some current process or from some future event. Risk is present in every aspect of our lives and many different disciplines focus on risk as it applies to them. From the IT security perspective, risk management is the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system. IT security risk is the harm to a process or the related information resulting from some purposeful or accidental event that negatively impacts the process or the related information.

One of the most widely used definitions of threat and threat-source can be found in the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems. NIST SP 800-30 provides the following definitions.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. Notice that the vulnerability can be a flaw or weakness in any aspect of the system. Vulnerabilities are not merely flaws in the technical protections provided by the system.

Significant vulnerabilities are often contained in the standard operating procedures that systems administrators perform, the process that the help desk uses to reset passwords or inadequate log review. Another area where vulnerabilities may be identified is at the policy level. For instance, a lack of a clearly defined security testing policy may be directly responsible for the lack of vulnerability scanning.

Here are a few examples of vulnerabilities related to contingency planning/ disaster recovery:

- Not having clearly defined contingency directives and procedures.
- Lack of a clearly defined, tested contingency plan.
- The absence of adequate formal contingency training.
- Lack of information (data and operating system) backups.
- Inadequate information system recovery procedures, for all processing areas (including networks).
- Not having alternate processing or storage sites.
- Not having alternate communication services.

The principle reason for managing risk in an organization is to protect the mission and assets of the organization. Therefore, risk management must be a management function rather than a technical function[1].

Quantitative Risk Assessment. Quantitative risk assessment draws upon methodologies used by financial institutions and insurance companies. By assigning values to information, systems, business processes, recovery costs, etc., impact, and therefore risk, can be measured in terms of direct and indirect costs.

Mathematically, quantitative risk can be expressed as Annualized Loss Expectancy (ALE). ALE is the expected monetary loss that can be expected for an asset due to a risk being realized over a one-year period.

$$ALE = SLE * ARO$$

Where:

- SLE (Single Loss Expectancy) is the value of a single loss of the asset. This may or may not be the entire asset. This is the impact of the loss.
- ARO (Annualized Rate of Occurrence) is how often the loss occurs. This is the likelihood.

Mathematically, this gets complicated very quickly, involving statistical techniques that are beyond the scope of this discussion. While utilizing quantitative risk assessment seems straightforward and logical, there are issues with using this approach with information systems. While the cost of a system may be easy to define, the indirect costs, such as value of the information, lost production activity and the cost to recover is imperfectly known at best. Moreover, the other major element of risk, likelihood, is often even less perfectly known [2].

Identifying Vulnerabilities. Specific vulnerabilities can be found by reviewing vendor web sites and public vulnerability archives, such as Common Vulnerabilities and Exposures (CVE - http://cve.mitre.org) or the National Vulnerability Database (NVD - http://nvd.nist.gov). If they exist, previous risk assessments and audit reports are the best place to start. Additionally, while the following tools and techniques are typically used to evaluate the effectiveness of controls, they can also be used to identify vulnerabilities:

- Vulnerability Scanners – Software that can examine an operating system, network application or code for known flaws by comparing the system (or system responses to known stimuli) to a database of flaw signatures.
- Penetration Testing – An attempt by human security analysts to exercise threats against the system. This includes operational vulnerabilities, such as social engineering.
- Audit of Operational and Management Controls – A thorough review of operational and management controls by comparing the current documentation to best practices against current documented processes. It is invaluable to have a base list of vulnerabilities that are always considered during every risk assessment in the organization. Moreover, vulnerabilities discovered during past assessments of the system should be included in all future assessments. Doing this allows management to understand that past risk management activities have been effective.

Communicating Risks and Risk Management Strategies. Risk must also be communicated. Once risk is understood, risks and risk management strategies must be clearly communicated to organizational management in terms easily understandable to organizational management. Managers are used to managing risk, they do it every day. So presenting risk in a way that they will understand is key. Ensure you do not try to use "fear, uncertainty and doubt." Instead, present risk in terms of likelihood and impact. The more concrete the terms are, the more likely organizational management will understand and accept the findings and recommendations.

With a quantitative risk assessment methodology, risk management decisions are typically based

on comparing the costs of the risk against the costs of risk management strategy. A return on investment (ROI) analysis is a powerful tool to include in the risk assessment report. This is a tool commonly used in business to justify taking or not taking a certain action. Managers are very familiar with using ROI to make decisions.

With a qualitative risk assessment methodology, the task is somewhat more difficult. While the cost of the strategies is usually well known, the cost of not implementing the strategies is not, which is why a qualitative and not a quantitative risk assessment was performed. Including a management-friendly description of the impact and likelihood with each risk and risk management strategy is extremely effective. Another effective strategic is showing the residual risk that would be effective after the risk management strategy was enacted [3].

Sample Risk Management **Tab.1**

Risk	Risk Description	Impact	Likelihood	Risk Mgmt Strategy	Cost	Residual Risk After Implementing Risk management Strategy
M[1]	Failure in environmental systems(e.g. air conditioning) Leaves systems unavailable.	Failure in environmental Controls could cause system to become unavailable for more than 48 hours.	Past data indicates this happens 1-2 times annually	Implement a hot spare at the alternate site	$ 250,000	L

3. Conclusion

In summary, successful and effective risk management is the basis of successful and effective IT security. Due to the reality of limited resources and nearly unlimited threats, a reasonable decision must be made concerning the allocation of resources to protect systems. Risk management practices allow the organization to protect information and business process commensurate with their value. To ensure the maximum value of risk management, it must be consistent and repeatable, while focusing on measurable reductions in risk. Establishing and utilizing an effective, high quality risk management process and basing the information security activities of the organization on this process will lead to an effective information security program in the organization.

References:

1. National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems (July 2002) – page 8.
2. National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems (July 2002) – page 12.
3. National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems (July 2002) – page 12.

ᲡᲐᲘᲜᲤᲝᲠᲛᲐᲪᲘᲝ ᲡᲘᲡᲢᲔᲛᲐ ᲓᲐ ᲠᲘᲡᲙᲘᲡ ᲛᲔᲜᲔᲯᲛᲔᲜᲢᲘᲡ ᲡᲢᲠᲐᲢᲔᲒᲘᲐ

თინათინ მშვიდობაძე
გორის სასწავლო უნივერსიტეტი, საქართველო

რეზიუმე

ნაშრომში წარმოდგენილია რისკის გააზრება. რისკის შეფასების მეთოდოლოგია მნიშვნელოვანი ფაქტორია ეფექტური უსაფრთხო კომპიუტერული გარემოს შესაქმნელად. სამწუხაროდ, საიფორმაციო ტექნოლოგიების სპეციალისტებისათვის ეს ჯერ კიდევ საყურადღებო სფეროა, რაც გამოწვეულია ტექნოლოგიებში ცვლილებების მაღალი დონით; ინტერნეტის მოხმარების მყისიერი ზრდით. ამის ფონზე, რისკის შეფასება გარდაუვალია (რეალობაა). ნაშრომში აღწერილია გამომწვევი საშიშროებებიც და მოცემულია რისკის მენეჯმენტის სტრატეგიები.

ИНФОРМАЦИОННАЯ СИСТЕМА И СТРАТЕГИИ МЕНЕДЖМЕНТА РИСКА

Мшвидобадзе Т.
Горийский Учебный Университет

Резюме

В работе представлено осмысление риска. Методология оценки риска является значительным фактором для создания эффективного безопасного компъютерного окружения. К сожалению, для специалистов информационных технологий эта сфера все еще требует внимания, что и вызвано высоким уровнем изменений в технологиях; ростом пользования интернетом. На этом фоне оценка риска является реалъностъю. В труде описаны вызывающие опасности и даны стратегии менеджмента риска.