5th International Quality Conference
May 20th 2011
Center for Quality, Faculty of Mechanical Engineering, University of Kragujevac

Miloš Petronijević[1)]
Ana Janković[1)]

1) Visoka tehnička škola Novi Beograd, Zorana Đinđića 152 A
2) Nomobbing, Kragujevac, Nenadovićeva 10

RISK MANAGEMENT THROUGH IT SECURITY TECHNOLOGY

Abstract: *Every organization has a mission. In this digital era, as organizations use automated information technology (IT) systems to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT-related risk.*

Keywords: *Risk, quality, management, importance, analisys*

1. INTRODUCTION

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. This guide describes the risk assessment process, which includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. Risk mitigation, which refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. The continual evaluation process and keys for implementing a successful risk management program. The DAA or system authorizing official is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk before authorizing (or accrediting) the IT system for operation.

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives. Take the case of home security, for example. Many people decide to have home security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of their property. Presumably, the homeowners have weighed the cost of system installation and monitoring against the value of their household goods and their family's safety, a fundamental "mission" need.

The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real-world threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

2. KEY ROLES

Risk management is a management responsibility. This section describes the key roles of the personnel who should support and participate in the risk management process.

Senior Management. Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.

Chief Information Officer (CIO). The CIO is responsible for the agency's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.

System and Information Owners. The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. Typically the system and information owners are responsible for changes to their IT systems. Thus, they usually have to approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.

Business and Functional Managers. The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper security for the IT systems, which, if managed properly, will provide mission effectiveness with a minimal expenditure of resources.

ISSO. IT security program managers and computer security officers are responsible for their organizations' security programs, including risk management. Therefore, they play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the IT systems that support their organizations' missions. ISSOs also act as major consultants in support of senior management to ensure that this activity takes place on an ongoing basis.

IT Security Practitioners. IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their IT systems. As changes occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational policies, introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems.

Security Awareness Trainers (Security/Subject Matter Professionals). The organization's personnel are the users of the IT systems. Use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users

3. SYSTEM CHARACTERIZATION

In assessing risks for an IT system, the first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.

The methodology described in this document can be applied to assessments of single or multiple, interrelated systems. In the latter case, it is important that the domain of interest and all interfaces and dependencies be well defined prior to applying the methodology.

Identifying risk for an IT system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:

Hardware Software System interfaces (e.g., internal and external connectivity) Data and information Persons who support and use the IT system System mission (e.g., the processes performed by the IT system) System and data criticality (e.g., the system's value or importance to an organization) System and data sensitivity. Additional information related to the operational environmental of the IT system and its data includes, but is not limited to, the following:

- The functional requirements of the IT system
- Users of the system (e.g., system users who provide technical support to the IT system; application users who use the IT system to perform business functions)
- System security policies governing the IT system (organizational policies, federal requirements, laws, industry practices)
- System security architecture
- Current network topology (e.g., network diagram)
- Information storage protection that safeguards system and data availability, integrity, and confidentiality
- Flow of information pertaining to the IT system (e.g., system interfaces, system input and output flowchart)
- Technical controls used for the IT system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
- Management controls used for the IT system (e.g., rules of behavior, security planning)
- Operational controls used for the IT system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
- Physical security environment of the IT system (e.g., facility security, data center policies)
- Environmental security implemented for the IT system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

The level of protection required to maintain system and data integrity, confidentiality, and availability.

For a system that is in the initiation or design phase, system information can be derived from the design or requirements document. For an IT system under development, it is necessary to define key security rules and attributes planned for the future IT system. System design documents and the system security plan can provide useful information about the security of an IT system that is in development.

For an operational IT system, data is collected about the IT system in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices. Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the IT system.

4. INFORMATION GATHERING TECHNIQUES

Any, or a combination, of the following techniques can be used in gathering information relevant to the IT system within its operational boundary:

Questionnaire. To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the IT system. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the IT system. The questionnaire could also be used during on-site visits and interviews.

- **On-site Interviews.** Interviews with IT system support and management personnel can enable risk assessment personnel to collect useful information about the IT system (e.g., how the system is operated and managed). On-site visits also allow risk

assessment personnel to observe and gather information about the physical, environmental, and operational security of the IT system. Appendix A contains sample interview questions asked during interviews with site personnel to achieve a better understanding of the operational characteristics of an organization. For systems still in the design phase, on-site visit would be face-to-face data gathering exercises and could provide the opportunity to evaluate the physical environment in which the IT system will operate.

Document Review. Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan, security policies) can provide good information about the security controls used by and planned for the IT system. An organization's mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.

Use of Automated Scanning Tool. Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s).

Information gathering can be conducted throughout the risk assessment process, from Step 1 (System Characterization) through Step 9 (Results Documentation).

Output from Step 1–Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundary

4.1 Vulnerability Sources

The technical and nontechnical ulnerabilities associated with an IT system's processing environment can be identified via the information-gathering techniques described in Section

A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific IT systems (e.g., a specific version of a specific operating system). The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities. Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following:

- Previous risk assessment documentation of the IT system assessed
- The IT system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports
- Vulnerability lists, such as the NIST I-CAT vulnerability database (http://icat.nist.gov)
  Security advisories, such as FedCIRC and the Department of Energy's Computer Incident Advisory Capability bulletins
- Vendor advisories
- Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
- Information Assurance Vulnerability Alerts and bulletins for military systems
- System software security analyses.

4.2 System Security Testing

Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the IT system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test). Test methods include– Automated vulnerability scanning tool Security test and evaluation (ST&E) Penetration testing.

The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g., system allows anonymous File Transfer Protocol [FTP], sendmail relaying). However, it should be noted that some of the potential vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements. Some of the "vulnerabilities" flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it. Thus, this test method may produce false positives.

ST&E is another technique that can be used in identifying IT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an IT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

Penetration testing can be used to complement the review of security controls and ensure that different facets of the IT system are secured. Penetration testing, when employed in the risk assessment process, can be used to assess an IT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes.

The NIST SP draft 800-42, Network Security Testing Overview, describes the methodology for network system testing and the use of automated tools.

The results of these types of optional security testing will help identify a system's vulnerabilities.

5. CONTROL ANALYSIS

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

Because the risk assessment report is not an audit report, some sites may prefer to address the identified vulnerabilities as observations instead of findings in the risk assessment report.

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment (Step 5 below), the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

5.1 Control Methods

Security controls encompass the use of technical and nontechnical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

5.2 Control Categories

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.

Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

Section 4.4 further explains these controls from the implementation standpoint. The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (e.g., controls are not in place or controls are not properly implemented)..

REFERENCES:

[1] www.best-management-practice.com/Risk-Management-MoR/

[2] www.hse.gov.uk/**risk**/

[3] ww.rmmag.com/

[4] www.rmahq.org/

[5] www.nonprofitris**k**.org/