Journal of Information Security, **2011, 2, 85-90**
doi:10.4236/jis.2011.22008 Published Online April 2011 (http://www.scirp.org/journal/jis)

Proposed Framework for Security Risk Assessment

Zakaria I. Saleh, Heba Refai, Ahmad Mashhour
Faculty of Computer Science and Information Systems, Yarmouk University, Jordan
Email: *drzaatreh@aim.com, Refai86@yahoo.com, mashhour_ahmad@yahoo.com*
Received November 28, 2010; *revised January* 11, 2011; *accepted April* 12, 2011

Abstract

Security risk assessment framework provides comprehensive structure for security risk analysis that would help uncover systems' threats and vulnerabilities. While security risk assessment is an important step in the security risk management process, this paper will focus only on the security risk assessment framework. Viewing issues that exist in a current framework, we have developed a new framework for security risk and vulnerabilities assessment by adding new components to the processes of the existing framework. The proposed framework will further enhance the outcome of the risk assessment, and improve the effectiveness of the current framework. To demonstrate the efficiency the proposed framework, a network security simulation as well as filed tests of an existing network where conducted.

Keywords: Security Risk, Vulnerabilities, Framework, Simulation

1. Introduction

The substantial usage of information and communication devices, and the increasing interconnectivity among systems and organizations, is exposing organizations for security risk and vulnerabilities, including intentional threat that would be associated to sabotage and vandalism. Therefore, there is a growing interest in applying risk analysis and risk management to eliminate security problems and protect networks.

Security Risk management is an ongoing process of identifying these risks and implementing planes to address them and risk assessment is the part of the ongoing risk management process that assigns relative priorities for mitigation plans and implementation [1]. Thus, a risk assessment framework is needed with an approach for categorizing and sharing information about the security risks of the information technology infrastructure. Furthermore, to establish useful framework for risk analysis we have to clearly identify the risks, it is not sufficient to refer to probabilities and expected values [2]. This paper will evaluate different frameworks that are being in use and then will develop an enhanced framework that will improve the outcome of the existing security risk assessment frameworks.

1.1. Overview of Vulnerabilities and Security Framework

System Vulnerabilities are defined as fault or weakness that reduces and limits system ability [3]. Assessing security risk is the initial step to evaluate and identify risks and consequences associated with vulnerabilities and provide basis for management to establish cost effective security program. The vulnerability analysis is a part of risk assessment process that focuses on methods for identifying vulnerabilities and implementing measures to mitigate the vulnerabilities, by implementing suitable protection and safeguard to maintain acceptable network security level and protect information. Many types of network attacks require a high degree of technical expertise and some may require significant financial resources to be carried successfully; however some attacks may be accomplished with few resources and little expertise.

Johnston (2004) defined a framework as structure upon or into which contents can be pit and further relates it to thoughts that are directed for a purpose. A security framework provides holistic structure for risk analysis covering both terminology on risk and vulnerabilities concepts and methodology for risk and vulnerabilities analysis for safety and security [2]. The natural of risks however, could include the possibility of threat event (e.g. flood, earthquake, and fire) that have impact on the organization's information asset as well as its physical structures [4]. In addition, the nature of information networks allows for an attack to be launched from anywhere in the world, making identifying the origins of an attack a major difficulty, if the attack is detected to start with [5].

1.2. Research Objectives

Secured networks and information systems assist organization in sharing its business in trustworthy way, helping organization to build strong relationship with customer, supplier and other business partner. Creating trust relationships through the security of information and by means of effective security controls will improve the cash flow and profitability of organization [6,7]. In addition, security risk assessment provides complete view on existing security risk and necessary security safeguard, and provides approach to security management with alternative solution for decision-making and basis for future change made in security measure [8]. Therefore, a proper and efficient security risk assessment will result in improved outcome. To prove the effectiveness of this framework I will use network security emulation to answer the following research questions, which include:

1) How effective is the proposed framework for security risk assessment?

2) Does criteria process have an impact on the security risk assessment?

3) Does the proposed security risk assessment have an impact on the security strategy development process?

1.3. Security Risk Assessment Overview

Security risk assessment is being defined as the process of evaluating security risks that is conducted identifies the required security measures [9]. The assessment is conducted at the very early stages of the system development as well as when there is change to information asset or its environment. The process includes the evaluations and analysis of all asset and processes related to the system to identifying the threat and vulnerabilities that could affect confidentiality, integrity or availability of the system, and setting required control to manage the risk [1]. Risk assessment is an essential element of risk management and to be effective, risk assessment must be an ongoing process. Depending on the purpose and the scope of security risk assessment it can be categorized into three types: (1) high level assessment that can be applied for system at design phase to identify security risks before implementation; (2) comprehensive assessment that can be used to evaluate the security risk of particular system in department to provide recommendation for improvement; (3) pre-production assessment conducted on new information system before it's rolled out or after there is major functional change [10].

1.4. Security Risk Assessment Frameworks

1) The iterative process of IT security management, which starts with assessing security risk and based on the assessment results, an appropriate security protection and safeguards would be implemented to maintain a secure protection framework as illustrated in **Figure 1** [1].

2) The national infrastructure protection plan risk management framework (NNIP-RM) is structured to promote continuous improvement to enhance critical infrastructure protection and key resource protection as shown in **Figure 2** [4].

3) Framework for information security culture, provides organizations with understanding of how to establish an information security culture to minimize risks posed by employee behavior regarding the use of information assets (**Figure 3**), where the interaction between information security components such as a policy and the behavior of employees would have an impact on the resulting information security culture [11].

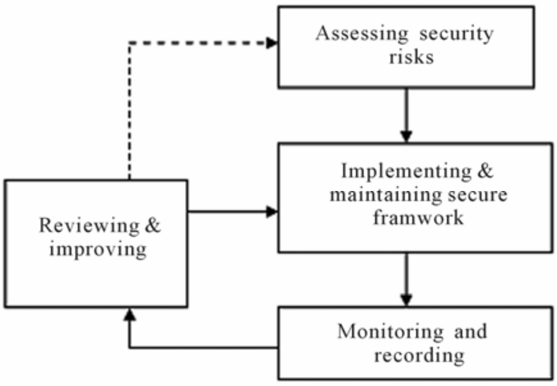

Figure 1. Security risk management process.

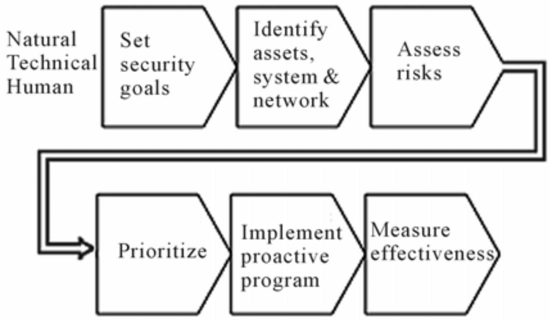

Figure 2. NIPP- RM framework.

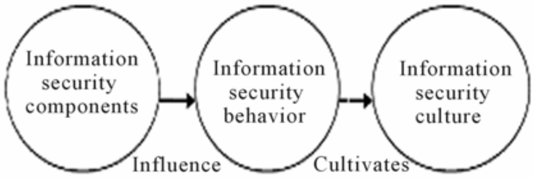
Information security components
Influence
Information security behavior
Cultivates
Information security culture

Figure 3. Information security culture framework.

2. Research Model

Security risk and vulnerabilities assessment has many benefits and challenges associated with it. The security risk assessment should provide complete view of the existing security risk and help provide alternative solution and changes to the security measures and controls. In light of that, this research believes that none of the discussed frameworks is fully providing the desired outcome. Therefore, we propose that an enhancement is needed, which will improve the security risk assessment process, and that enhancement can be made to Ogesio [1] security risk management approach (see **Figure 1**). The approach should include two more components which will be added and placed as process 2 (Identify infrastructure vulnerabilities) and process 3 (Analyze Risks & Vulnerabilities) to the existing security risk assessment process as being illustrated in **Figure 4**.

Network infrastructure vulnerabilities are the core of all technical security issues in any information systems. The extreme importance of infrastructures to modern network systems shall be recognized. These infrastructures are complex and interdependent; therefore protecting the infrastructures is an enormous challenge. Recognizing that an organization cannot afford the costs associated with absolute protection, it is necessary to identify and prioritize the vulnerabilities in these infrastructures. These vulnerabilities can affect everything running on the network. The information infrastructure now a day is still regarded as an easy and vulnerable entry point. But discovering the threat and the likely nature of an attack — remains difficult [5]. Therefore, infrastructure vulnerabilities and infra structure evolution requires effective crisis management and preventive, strategic planning, to try and eliminate them whenever possible. This requires an evaluation of the information infrastructure, where the main operational components of the information technology infrastructure are examined for weaknesses and technology vulnerabilities. Any basic risk assessment would identify and quantify this vulnerability.

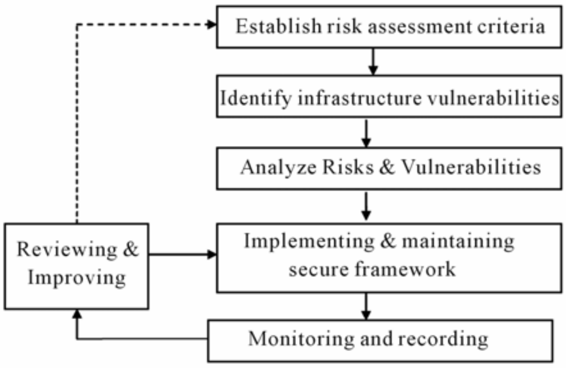
Establish risk assessment criteria
Identify infrastructure vulnerabilities
Analyze Risks & Vulnerabilities
Reviewing & Improving
Implementing & maintaining secure framework
Monitoring and recording

Figure 4. Proposed framework for security risk and vulnerabilities assessment.

However, establishing risk assessment criteria and then implementing & maintaining secure framework before Identify infrastructure vulnerabilities and analyze risks & vulnerabilities will not be as efficient as it would be desired.

Infrastructures vulnerabilities might arise from the common links where failures might propagate through the different systems. Thus, intrusion and disruption in one subsystem might provoke unexpected threats to other subsystem. There are four types Infrastructure threat (see **Table 1**), where attacks on the systems in all four types involve the malicious use of the information infrastructure either as a target or as a tool [12].

3. Research Method

The proposed framework effectiveness will be tested using SpiceWorks network management software version 4.7 (see **Figure 5**). SpiceWorks is a complete network management software, helpdesk, and PC inventory tools designed to manage networks in small & medium businesses. SpiceWorks gets a full and accurate scan of all network devices including Windows, Mac, and Linux machines and keep track of the network assets, run a helpdesk, monitor activity, receive reports and trouble-

Table 1. Infrastructure threat matrix [12].

		Target	
Means/Tool		Physical	Cyber
	Physical	1) - Severing a telecom cable with a backhoe - Smashing a server with a hammer - Bombing the electric grid	2) - Use of electromagnetic pulse and radio-frequency weapons to destabilize electronic components
	Cyber	3) - Hacking into a SCADA system that controls municipal sewage - “Spoofing” an air traffic control system to bring down a plane	4) - Hacking into a critical government network - Trojan horse in public switched network

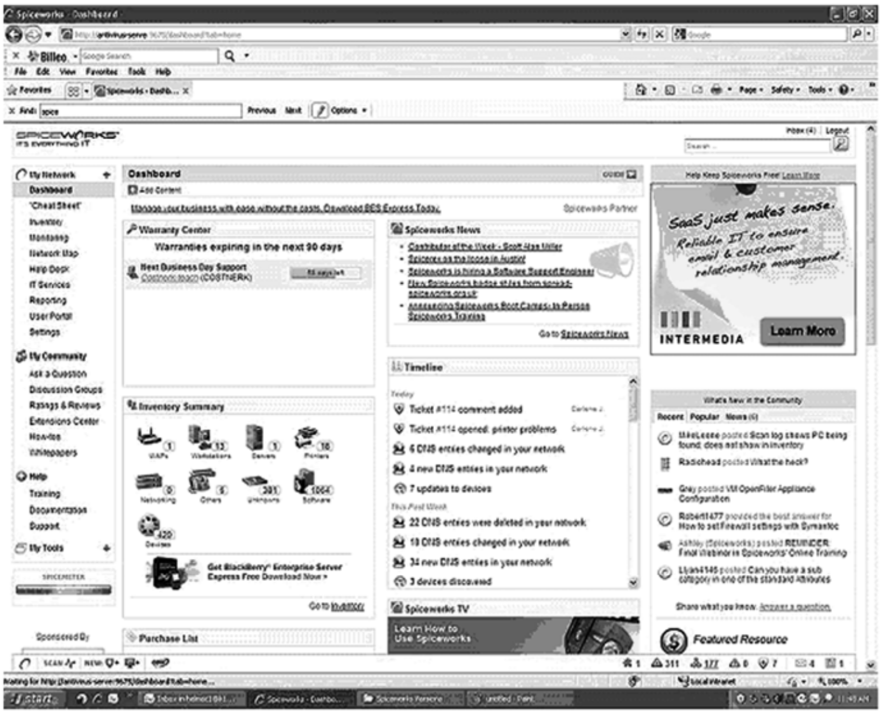

Figure 5. Spiceworks 4.7 screenshot.

shoot network problems [13]. The software will be used to test the network of a university (for security and privacy reasons, the name of the university will remain anonymous). Using SpiceWorks, we will implement Ogesio framework process [1] and the proposed framework, test a network, and then compare the findings.

4. Data Collection and Analysis

SpiceWorks network management software was installed and to test the network and to identify infrastructure vulnerabilities and analyze risks if any found (process 2 & 3). Evaluating the major events that were taking place in the network systems by applications and other devices, the evaluation revealed a number of audit failure, warnings and errors as displayed in **Figure 6.**

The ID of the system where the audit failures occur is displayed in **Table 2** along with the source of failure, event count, and the location and the time/date in which the failures occur.

The warnings are listed in **Table 3**, along with the ID of the applications that may failure or error occur on it, source of these expected errors, the event count, the systems involved and the time/date of warning.

The security issues are listed in **Table 4**, along with the ID of the systems where the errors occur, source of errors, event count, the systems involved, and the time/date that the errors occur. In addition, **Table 4** displays the type of security issues and the device (name or address) where the issue is identified.

Analyzing **Tables 2**, **3** and **4**, we can specify the likelihood of the events to occur by looking at the count

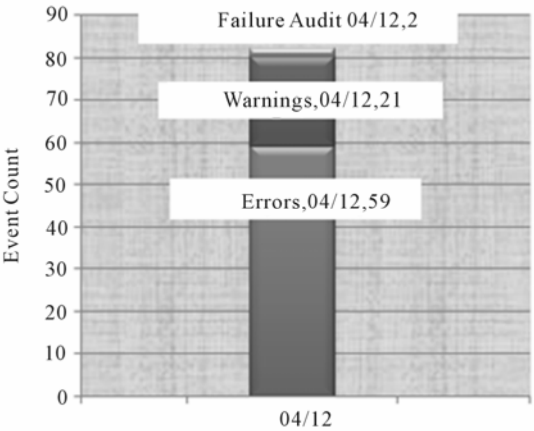

Figure 6. The major events in the network.

Table 2. Audit failure report.

ID	Sources	Count	Computers	4/12/2010
4001	SWService	2	Srvs	18:07:32

Table 3. Warnings report.

ID	Sources	Count	Computers	4/12/2010
8032	BROWSER	3	Srvs	20:59:43
8021	BROWSER	3	Srvs	20:57:19
7000	Service Control Manager	2	Srvs	20:55:22
20	Print	1	Srvs	20:12:55
7034	Service Control Manager	4	Srvs	20:08:48
7031	Service Control Manager	3	Srvs	20:03:35
7001	Service Control Manager	12	Srvs	19:51:21
7022	Service Control Manager	11	Srvs	19:51:21
7032	Service Control Manager	1	Srvs	19:15:09

Table 4. Security issues report.

ID	Sources	Count	Computers	4/12/2010
1	WinVNC4	5	Srvs	21:15:47
107	Report Server Windows Service	2	Srvs	20:54:55
18456	MSSQLSERVER	2	Srvs	20:54:53
3	SQL Browser	4	Srvs	20:54:00
1001	MS Installer	3	Srvs	20:26:15
0	System Service Model Install 3.0.0.0	10	Srvs	20:17:05
0	Net Runtime	14	Srvs	20:08:47

column that specifies how many time this event was repeated and reported. For example, we can conclude that most of the errors events have high likelihood of occurrence, and some of the warning event has high likelihood and some warnings have medium likelihood of occurrence, but the audit failure has low likelihood of occurrence because the event count is only 2.

Errors were also reported during the system test (see **Table 5**). In light of that, we need to assess the impact of the errors and warnings on the critical data assets to develop the appropriate method to manage the risks and to protect data assets. For example, an effective firewall provides the software or hardware necessary to validate and authenticate traffic and user against a security policy or set of rules to allow them to pass the private or trusted side of network. Firewall problems and issues could mean that external unauthorized people can access the private network and disclose sensitive and critical data asset.

Table 5. Reported errors type.

Device Name	Error
172.19.150.127	Permission or Firewall Problem
okhreis-pc	Permission or Firewall Problem
172.19.150.74	Permission or Firewall Problem
yu-9c2f5e2e9e4b	Permission or Firewall Problem
172.19.150.58	Permission or Firewall Problem
dr-y-aaage	Permission or Firewall Problem
drsalah	Permission or Firewall Problem

5. Conclusions

Based on the results and the findings, we conclude that the framework process is providing the desired results, where each process depends on the result of the previous one. For example, during the tests, we have identified warnings and security issues. Unless the two proposed components are added to the existing security risk assessment process as illustrated in **Figure 4** (process 2: Identify infrastructure vulnerabilities) and (process 3: Analyze Risks & Vulnerabilities) those warnings may become real issues and introduce new vulnerabilities soon or later. The only way to confirm that they will (or will not), is by identifying the vulnerabilities that each warning may have, and then analyzing the risk associated with it. Therefore, the risk analysis process depends on the result of the infrastructure vulnerabilities identification, where in this process the vulnerabilities are identified, and then the risk is analyzed based on its impact and probability of occurrence. The monitoring process is based on the result of the established risk assessment criteria, where reports are produced to indicate all alerts or warning of all possible threats. The monitoring is continuously repeated to insure the development of effective security system, and an appropriate action is taken to handle the risks associated with those threats, which should result in improving the security system. In addition, the risk assessment criteria should be based on the result of the reporting process. In other words, manager will use the report that summarize the status and performance of the security in the organization, and based on that, management will update the security system (and policy) to eliminate security weakness, and thus enhance the security system.

In light of the findings, we can conclude that the framework is effective for security risk assessment because the processes are proven to be highly interacted with each other. We also conclude that the risk assessment criteria process has appositive impact on security risk assessment, as the test results have shown in the different stages of the process. In addition, the security risk assessment process has a positive impact on the security strategic development, through continuous development of the security system to improve the security system. The security plan and strategies may specify the priorities and area of concerns as well as the degree of risk that management can accept, however, without applying the added process the system may not be as effective, as the results indicate.

6. References

[1] The Office of the Government Chief Information Officer, "Security Risk Assessment and Audit Guidelines", 2009. http://www.ogcio.gov.hk/eng/prodev/download/g51_pub

[2] T. Even, "A Unified Framework For Risk and Vulnerability Analysis Covering Both Safety and Security", *Reliability Engineering and System Safety*, Vol. 92, No. 6, 2007, pp. 745-754. doi:10.1016/j.ress.2006.03.008

[3] G. Stoneburner, A. Goguen, A. Feringa, "Risk Management Guide for Information Technology Systems", 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30f

[4] Homeland Security, "National Infrastructure Protection Plane Risk Management Framework", (2009). http://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt

[5] M. D. Cavelty, "Critical Information Infrastructure: Vulnerabilities, Threats and Responses" *Disarmament Forum ICTs and International Security*, No. 3, 2007, pp. 15-22.

[6] R. Olsson, "In Search of Opportunity Management: Is the Risk Management Process Enough?" *International Journal of Project Management*, Vol. 25, No. 8, November 2007, pp. 745-752. doi:10.1016/j.ijproman.2007.03.005

[7] S. Posthumus, R. Solms, "A Framework for the Governance of Information Security", *Computer and Security*, Vol. 23, No. 8, December 2004, pp. 638-646. doi:10.1016/j.cose.2004.10.006

[8] Akelainc, "What Risk and Vulnerability Assessment", 2009. http://www.akelainc.com/pdf_files/What%20is%20risk%20and%20vulnerability%20assessment.pdf

[9] Insight Networking, "Risk and Vulnerabilities Assessment", 2009. https://images01.insight.com/media/pdf/IN_RVA_Datasheet

[10] S. Bajpai, A. Sachdeva, J. Gupta, "Security Risk Assessment: Applying the Concept of Fuzzy Logic", *Journal of Hazardous Materials*, Vol. 173, No. 1-3, January 2010, pp.258-264. doi:10.1016/j.jhazmat.2009.08.078

[11] A. Veiga, J. Eloff, "A Framework and Assessment for Information Security Culture", *Computer and Security*, Vol. 29, No. 2, March 2010, pp. 196-207. doi:10.1016/j.cose.2009.09.002

[12] Dunn Myriam, "A Comparative Analysis of Cyber security Initiatives Worldwide", *WSIS Thematic Meeting on Cybersecurity*, Geneva, 28 June-1 July 2005.

[13] SpiceWorks Inc., "SpiceWorks, IT Is Everything", April 14, 2010. http://www.spiceworks.com/