Information Security Risk Assessment

Introduction

Information security risk assessment is an on-going process of discovering, correcting and preventing security problems. The risk assessment is an integral part of a risk management process designed to provide appropriate levels of security for information systems. Information security risk assessments are part of sound security practices.

Purpose

The purpose of the risk assessment is to identify threats and vulnerabilities related to your organization.

Scope

The scope of this risk assessment encompasses the potential risks and vulnerabilities to the **confidentiality**, **availability** and **integrity** of all systems and data that your organization creates, receives, maintains, or transmits.
Information is gathered through a web interface, phone, email and an onsite visit. After discovery and analysis, you will receive a document with a summary and recommendations.

Methodology

We follow the Industry Standard Guidelines set forth by NIST (National Institute of Standards and Technology) Special Publication 800-30 Revision 1.

The asset audit approach towards risk assessment looks at the assets the organization has and determines if each asset is being protected adequately. Typically, an asset audit process will include the following steps:

a. **Information asset identification** – Identifying all the data that the system being assessed stores, processes, transmits or has access to. The data can include company files, backup druves, and customer information.
b. **Data flow** – Determines the means by which each information asset identified arrives, is stored on, and leaves the system.
c. **Threat analysis** – Determines the different threat mechanisms that can be used to acquire the information as the data

- Enters the system
- Is stored on the system
- Leaves the system

d. **Likelihood of threat occurrence** – determines how likely each threat mechanism identified will happen

e. **Impact Analysis** – Assess the impact of data being disclosed, corrupted or destroyed or unavailable for a certain period of time
f. **Safeguard identification** – Selects the relevant safeguards or controls that needs to be implemented to protect the organization's information assets. These controls can be technical (e.g. install personal firewalls on all remote users' computers) or non-technical (e.g. acceptable use policy or security awareness training programs)

Risk = Threat Likelihood x Magnitude of Impact

Authoritative Sources

NIST SP 800- 30 Risk Management Guide for Information Technology Systems
NIST SP 800- 37 Guide for Applying the Risk Management Framework to Information Systems
NIST SP 800- 39 Managing Information Security Risk

Vulnerability Sources

- SANS Top 20 (www.sans.org/top20/)
- OWASP Top 10 (www.owasp.org/documentation/topten.html)
- NIST I-CAT vulnerability database (icat.nist.gov)
- Microsoft Security Advisories(www.microsoft.com/security)
- CA Alert service (www3.ca.com/securityadvisor)
- OTX and other Open Source Threat databases

Vulnerability Scan

During the assessment our technician will conduct a **PASSIVE** Vulnerability Scan to help us build a profile of your organizations' potential vulnerabilities. During this scan **none** of your information will be accessed nor at any time will we have access to any computer system. The scanner probes all your computers to find any known vulnerabilities. The scan takes from 15 minutes to an hour depending on how many computers are on your network. We will need your written permission to run the scan. You will be provided a detailed report on the scan results.

WARNING AND DISCLAIMER

Every effort has been made to make this document, subsequent documents and the Risk Assessment Report we provide as complete and as accurate as possible. No warranty or fitness is implied. The information gathered is partly supplied by your company and we cannot verify the accuracy of every statement. Silloway Networks, Inc. shall have neither liability nor responsibility to any person or entity with respect to any losses or damages arising from the reliance to the information contained in the final report. **The Risk Assessment in NOT a guarantee that you will never have a security issue, suffer a cyber-attack, or that malicious software will be installed by a hacker, phishing attempt, by one of your employees, or any other known or unknown attack vector.**