DETAILED RISK ASSESSMENT REPORT

Executive Summary

During the period March 27, 2012 to April 23, 2012 a detailed information security risk assessment was performed on New Life Medical's information technology lab ("NLITL").

NLITL processes the medical records and stores them on a file server as Adobe PDF documents. Employees of NLlTL have admitted to installing file sharing applications on company computers. There is no policy on the use of such applications.

The assessment identified several high to medium risk items related to the installation of file sharing applications on company machines. These risks should be addressed by management.

DETAILED ASSESSMENT

1. Introduction

a. Purpose

The purpose of the risk assessment was to identify threats and vulnerabilities related to the installation of file sharing applications on company computers located at the New Life Information Technology Lab (“NLITL”). The computers in question process medical insurance records and then store them on a file server as Adobe PDF documents. This risk assessment is conducted in fulfillment of the requirements for lab 3.

b. Scope

The New Life Information Technology Lab comprises several components. The company has 30 employees in which use PCs that process and edit medical records using Adobe Acrobat Professional. The employees all have access to the internet and some of the employees admitted to installing fill sharing applications on their workstations. The company also has a server in which serves files over their internal network. The employees access two shared directories and share a password for them. NLITL also has a company website in which allows customers to upload PDF documents.

The scope of this assessment includes all the components described above.

2. Risk Assessment Approach

a. Techniques Used

Technique	Description
Employee interviews	The risk assessment teams conducted interviews with employees who admitted to downloading file sharing programs on company computers. The risk assessment team also interviewed the operations manager to help identify any adverse effects of the applications.
Assessment tools	The team used several security testing tools in which reviewed system configurations and tested for vulnerabilities within the companies system. The tools used where Nmap, Nessus, and AppScan.
Site visit	The team conducted a site visit and evaluated company protocols.
Vulnerability sources	The team accessed a verity of sources to help identify vulnerability. The sources consulted included: • SANS Reading Room (http://www.sans.org/reading_room/) • Security Focus Archive (http://www.securityfocus.com/archive/) • CVE Vulnerability List (www.cvedetails.com/vulnerability-list//) • Secunia Advisories (http://secunia.com/advisorie) • Adobe Security Bulletins (http://www.adobe.com/support/security/bulletins/)

b. Risk Model

In determining risks associated with file sharing applications installed on company computers we utilized the following model for classifying risk:

Risk = Likelihood X Magnitude of Impact

And the following definitions:

Threat Likelihood

Likelihood (Weight Factor)	Definition
High: 1.0	Threat source is highly motivated and sufficiently capable, and no controls exist to prevent exploitation.
Medium: 0.5	Threat source is highly motivated and capable, but controls exist that may prevent exploitation.
Low: 0.1	Threat source lacks motivation or capability, or effective controls exist.

Magnitude of Impact

Impact (Score)	Definition
High: 100	The loss of confidentiality, integrity, or availability could be expected to have a major or catastrophic adverse effect on the organizational operations, assists, or individuals. Examples: • A severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions • Major damage to organizational assets • Major financial loss • Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Medium: 50	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Examples: • Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced • Significant damage to organizational assets • Significant financial loss • Significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low: 10	The loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals. Examples: • Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced • Minor damage to organizational assets • Minor financial loss • Minor harm to individuals.

Risk was calculated as follows:

		Threat Likelihood		
		Low (10)	Medium (50)	High (100)
Impact	Low (0.1)	Low Risk (10 x 0.1 = 1)	Low Risk (50 x 0.1 = 5)	Low Risk (100 x 0.1 = 10)
	Medium (0.5)	Low Risk (10 x 0.5 = 5)	Medium Risk (50 x 0.5 = 25)	Medium Risk (100 x 0.5 = 50)
	High (1.0)	Low Risk (10 x 1.0 = 10)	Medium Risk (50 x 1.0 = 50)	High Risk (100 x 1.0 = 100)

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

3. System Characterization

a. Technology components

The employees at NLITL use Dell PCs in which run Windows 2000. All employees have Adobe Acrobat Professional version 9 installed in order to create and edit medical records. In addition some of the employees have installed file sharing applications on their machines .The employees use Internet Explorer version 6 and access any website unrestricted. The company has a single server that is used for file storage and hosts the company's web site. This server runs Ubuntu version 9 and uses Samba to serve files on an internal network .Share- level security is implemented and there are only two shared directories in which every employee knows the password for.

NLITL's company web site allows customers to upload PDF documents and its web server is Oracle Web Logic Server version 10. No security training program has been implemented and employees are not technically competent.

4. Vulnerability Statement

The following potential vulnerabilities were identified:

Vulnerability	Description
Buffer over flow	Microsoft Windows 2000 is vulnerable to buffer overflows. While writing data to buffers a malicious program unintentionally downloaded by file sharing can overrun the buffer's boundary on critical system components and execute code throughout the system. Oracle WebLogic 10 also can also be compromised by a buffer overflow leaving the server at the mercy of the attacker.
Trojan Horse viruses	Due to the popularity and peer to peer capabilities file sharing applications prime sources of Trojan viruses.
Spyware	File sharing applications can download spyware from within the interface or have it embedded within the application.
Unsecure password protocol	Employees share one password to access the company's directory. A malicious application downloaded through file sharing applications can use this password to access the companies' directories.
Remote code execution	By simply visiting a malicious web site internet explorer 6 can allow remote code to be executed from an outside source. A Trojan downloaded by file sharing can simply redirect the user to a malicious site and control company machines.
Remote administration	Adobe Acrobat 9 Professional can potentially allow remote administration to an outside source. Malicious applications downloaded by file sharing can easily take advantage of this. Samara ran on Ubuntu 9 can potentially remotely run programs as administrator as well and is therefore at equal risk. In addition to the above risks file sharing applications can be used to install a remote administration tool (RAT) and provide total control to an attacker.
Lack of security training	The employees lack any sort of Information security training. This makes it simple for them to be targeted by malicious users on a peer to peer network.
Phishing attacks	Phishing emails have been sent specifically company. This is concern for sensitive information leaking to information harvesters.
Lack of Content Filters	Employees have unrestricted access to the internet. This paves the way for Spyware, phishing, and Trojans.

5. Threat Statement

The team identified the following threat-sources and associated threat actions applicable to NLITL:

Threat-Source	Threat Actions
Hacker	• Web defacement • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer Criminal	• Identity theft • Spoofing • System intrusion • Information harvesting
Insiders (dishonest employees, poorly trained employees, or terminated employees)	• Browsing of personally identifiable information • Malicious code (e.g., virus) • System bugs • Unauthorized system access

6. Risk Assessment Results

Item Number	Observation	Threat-Source Vulnerability	Existing Controls	Likelihood	Impact	Risk Rating	Recommended controls
1	Buffer overflows initiated by malicious applications compromise the company machines.	Hackers/Computer Criminals	none	Medium	High	Medium	Update all critical components of the system to the latest version. Proper logging protocols should be in place to insure operations are running in the norm.
2	Employees unknowingly downloaded Trojan viruses on companies machines	Hackers/ poorly trained employees	none	High	High	High	Restore and update all components of the system. Content filtering should be in place to prevent employees from downloading Trojans. There should also be a threat management system or application integrated into the system.
3	Spyware downloaded by peer to peer program harvested information from both employees and customers.	Computer Criminals/ identity theft/ poorly trained employees	Share level protection	Medium	High	Medium	A threat management system or application should be in place. User level authentication and a string password protocol would help to inhibit information harvesting.
4	Phishing attempts made directly to the company.	Computer Criminals/ poorly trained employees	none	High	Medium	Medium	Proper training for employees should be practiced to ensure phishing attempts remain futile. Content blocking should be implemented to ensure legitimate sites are accessed.
5	Employees leak the company password to a phishing attack.	Insiders/Computer Criminals	none	Medium	High	Medium	Employees need to be trained to identify phishing attempts as well as provided user level authentication and strong password protocols.

6	A Trojan program downloaded by file sharing applications takes control of the company server and machines.	Hackers/ System intrusion	Share level protection	Medium	High	Medium	Intergraded threat management should be implemented as well a protocol regarding applications allowed on company machines. Training should insure employees follow the company protocol.
7	A system intrusion goes unnoticed by employees for an extended period of time	Improperly trained employees.	none	High	High	High	Employees should be trained and fully aware of normal operations that are performed by the company system. Any change in this routine should be presented to the management.
8	An employee is redirected to a site in which then compromises the system	Computer criminal/ system intrusion	Share level protection	Medium	High	Medium	Content filters should be in place to insure employees do not get directed to a malicious site. The web browser should also be upgraded to the latest version.
9	An employee downloads illegal or copyrighted content causing huge legal penalties.	Insider/ poorly trained employees	none	High	High	High	Outside file sharing applications should be prohibited and content filters in place to prevent employees from knowingly or unknowingly downloading illegal or copyrighted content. Employees should also be aware of the penalties for such actions and have it clearly expressed in the company policy.