10

Department of Electrical and Computer Engineering
University of Victoria

SENG 460 – Practice of Information Security and Privacy

Assignment 3

Case Study: Security Threat Risk Assessment

1.0 Background Information/Scenario:

The university's IT department has decided that it would be a prudent measure to conduct a security threat risk assessment for their web environment so they could gain an understanding of their vulnerabilities and lay the groundwork for designing and applying effective controls for future web services. They are not sure where to start, considering that there are many apparent weaknesses in their system of controls. They are not sure which threats to address and in what order because they seem to be in an unstable environment. They don't have a good handle on their assets nor the value of the assets. As a result, they find themselves facing a great deal of uncertainty without clear priorities and are unsure of that safeguards will be justified in the end. What steps should they take, and in what order, to start them in the path to design effective and efficient web environment controls?

2.0 Preparation Phase

The Security Threat Risk Assessment (STRA) for the university will assess the current and attempt to predict future vulnerabilities of the IT system in relation to their web environment. The STRA will develop this assessment by:

1. Identifying the assets that are currently of value in relation to the web interface (be it direct value, or value indicated through a compromised system).
2. Based on the assets, a Threat Assessment will be developed.
3. From there, a Risk Assessment is developed which will be categorized based on a vulnerability assessment and a calculation of residual risk.
4. A Recommendation Phase will then outline ways to mitigate the threats uncovered based on importance.

This scope of this report is limited to only the web environment in use at the university. Assessments outside the scope of the web environment are not within the mandate of this report.

This STRA will be developed by Neven Colak. Neven Colak has no experience writing STRA reports. Although a fairly bright individual, the universities IT department should not consider the results of this report as the final word in its STRA. Please use this report as a stepping stone to protect the web environment, and nothing more. Neven Colak assumes no liability for the use of this document as anything more than an exercise in developing a STRA.

In order to facilitate the creation of this report, information was requested that could help to complete an overall assessment. Unfortunately, the universities IT department has provided no additional information, no asset information, or value of assets, and no reports or documentation to supplement this report. As such, this report shall be considered preliminary until such time that more information becomes accessible to the author, at which time a new STRA can be developed based on this information.

This report will be completed and submitted to the university on January 31, 2014. It will contain the four deliverables as outline on the previous page. Although the report and recommendations will be provided, the implementation of the report is at the discretion of the university, as well as any budgetary considerations resulting from the recommendations provided.

2.1 Asset Identification Phase

Based on the TRA-1 Methodology the following table outlines the assets considered in this STRA.

Table 1: Asset Valuation Table

University				Asset Value				
Class	**Category**	**Group**	**Sub-Group**	**Confid.**	**Avail Int**	**Avail Op**	**Integrity**	**$**
People	Employees	IT Staff	Systems Administrators		HIGH	FB		
Tangible	Information	Personal Data	Employees	HIGH	HIGH		HIGH	
Tangible	Information	Personal Data	Clients	HIGH	HIGH		HIGH	
Tangible	Information	Financial Records	Payroll	HIGH	HIGH		HIGH	
Tangible	Hardware	Network Components	Routers		MEDIUM			
Tangible	Software	Security Utilities	Encryption Packages		LOW			
Tangible	Facilities	Buildings	Data Centres		HIGH			

Table 1 was developed using the Harmonized Threat and Risk Assessment TRA-1 asset listing (Appendix B-2 in the TRA-1 Methodology), which contains various assets that can be applied to the STRA in development.

Once the Assets have been taken into consideration, the Asset Value is determined using Appendix B-5 in the TRA-1. This section states "Based upon the maximum injury levels that could reasonably be expected to arise in the event of a compromise to their confidentiality (C), availability (A) and integrity (I), insert the relevant asset values determined in accordance with the Expanded Injury Table in Appendix B-4 ranging from Very Low through Very High (VL through VH). In cases where personal safety is a potential concern, assign both intrinsic (i) and operational (o) availability values for the affected personnel."[1]

Note that Appendix B-4 in the TRA-1 concerns itself with the injury to personnel due to various degrees of threat involved.

[1] http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-b5-eng.doc January 31, 2014

2.2 Threat Assessment Phase

Based on the assets listed in Table 1, the following Threat Assessment Table is created to anticipate plausible and realistic threats that could affect these assets. The asset sub group affecting all the elements in Table 1 is the Universities IT Department.

Table 2: Threat Assessment Table

Asset Assessed:								Threat Levels Affecting		
ID No.	Class	Activity	Agent Category	Agent	Event	Likelihood	Gravity	Confid.	Avail.	Integrity
5	Deliberate	Espionage	Hostile Intelligence Service	Services	Network Exploitation	HIGH	HIGH	VERY HIGH	-	-
19	Deliberate	Espionage	Industrial Espionage	Companies	Reverse Engineering	LOW	MEDIUM	LOW	-	-
36	Deliberate	Sabotage	Disgruntled Employees	Groups/Individuals	Delete/Destroy Records	HIGH	HIGH	-	VERY HIGH	-
46	Deliberate	Sabotage	Hackers	Wannabees	Denial of Service Attacks	HIGH	MEDIUM	-	HIGH	-
102	Deliberate	Sabotage	Organized Crime	Groups	Identity Theft	HIGH	HIGH	VERY HIGH	-	-
126	Accidents	Office Accidents	Employees	Cleaning Staff	Unplug Equipment	MEDIUM	MEDIUM	-	-	MEDIUM
134	Accidents	Software Errors	System Administrators	Individuals	Software Configuration Errors	MEDIUM	MEDIUM	-	-	MEDIUM
136	Accidents	Hardware Failures	Hardware Vendors	Companies	Equipment Malfunction	MEDIUM	HIGH	-	HIGH	-
197	Natural Hazards	Earth Movement	Earthquakes	Interplate Earthquake	Moderate (5.0-5.9)	LOW	HIGH	-	MEDIUM	-

The above table shows a listing of various threats that will be considered as risks to the universities web environment. TRA-1 Tables C-1 (Threat Likelihood Table), C-2 (Threat Gravity Table), and C-3 (Threat Levels Table) were used after the threats where assigned to determine the degree of threat to the web environment for each instance.

2.3 Risk Assessment Phase

With the Assets gathered and potential risks determined, the next step in the process is to determine the risk to the web environment based on the information gathered.

3

2.3.1 Vulnerability Assessment

Table 3: Vulnerability Assessment Table

Vulnerability Class	Vulnerability Group	Vulnerability	Related Vulnerability	Level	Asset Exposed	Threat Facilitated
IT Security	Technical Safeguards	Software Integrity	Malicious Code Protection	HIGH	Personal Data, Financial Records, Security Utilities	Hostile Intelligence Service
IT Security	Technical Safeguards	Software Integrity	Malicious Code Protection	HIGH	Personal Data, Financial Records, Security Utilities	Industrial Espionage
Physical Security	Destruction	Destruction Equipment: IT Media	Destruction Equipment: Paper	MEDIUM	Network Components	Disgruntled Employees
IT Security	Technical Safeguards	Software Integrity	Malicious Code Protection	HIGH	Personal Data, Financial Records, Security Utilities	Hackers
IT Security	Technical Safeguards	Software Integrity	Malicious Code Protection	HIGH	Personal Data, Financial Records, Security Utilities	Organized Crime
Physical Security	Access Controls	Identification Cards	Electronic Access Controls	LOW	Buildings, IT Staff	Employees
Security Screening	Reliability Status	Regular Updating	Evaluating Results	LOW	Personal Data, Financial Records	System Administrators
IT Security	Technical Safeguards	Backup/Recovery		HIGH	Network Components	Hardware Vendors
Security in Emergencies	Plans and Procedures	Departmental Plans		MEDIUM	Buildings, IT Staff	Earthquakes

Table 3 utilizes TRA-1's Appendix D-3, which outline the vulnerability metrics used to determine the level of severity for each vulnerability class. The items taken into account are the probability of prevention, the severity of the outcome, then using those metrics to determine the overall vulnerability. This table takes some liberal viewpoints such as assuming the current states of some vulnerabilities are not adequate. For example, for *Software Integrity*, the assumption is made that the current state is moderately effective, giving that a MEDIUM preventative score (Table D3-1 in TRA-1), however the severity of an intrusion would be classified as HIGH (Table D3-2, in TRA-1), giving an overall HIGH Level of Vulnerability (From Table D3-3). All other Levels are found in a similar manner.

This table is based on information provided by the customer, as no information has been provided, the entries would be re-evaluated as more information becomes available.

2.3.2 Calculation of Residual Risk

Utilizing the information developed to this point, a prioritized assessment can determine the residual risk which can be used during the recommendation phase for developing areas to work on.

Using Table E-1 (Numeric Scores for Asset Value, Threat and Vulnerability Levels) and Table E-2 (Risk Levels and Ranges) in the TRA-1 as well as the formula:

$$\text{Residual Risk} = \text{Asset Value} \times \text{Threat} \times \text{Vulnerability}$$

A Residual Risk score was determined for each Threat, Vulnerability and Asset. The following table shows the outcome.

Table 4: List of Assessed Residual Risks

Asset	Asset Values			Associated Threat	T	Related Vulnerability	V	Residual Risk	R
(Group/Subgroup)	C	A	I	(Activity/Agent Category)				($A_{Val} \times T \times V$)	
IT Staff		HIGH		Office Accidents	MEDIUM	Regular Updating	LOW	24	MEDIUM
		HIGH		Earth Movement	MEDIUM	Backup/Recovery	HIGH	48	HIGH
Personal Data/Employees	HIGH	HIGH	HIGH	Sabotage	VERY HIGH	Software Integrity	HIGH	80	VERY HIGH
	HIGH	HIGH	HIGH	Espionage	LOW	Software Integrity	HIGH	32	MEDIUM
Personal Data/Clients	HIGH	HIGH	HIGH	Sabotage	VERY HIGH	Software Integrity	HIGH	80	VERY HIGH
	HIGH	HIGH	HIGH	Espionage	LOW	Software Integrity	HIGH	32	MEDIUM
Financial Records		HIGH		Sabotage	VERY HIGH	Software Integrity	HIGH	80	VERY HIGH
		HIGH		Espionage	LOW	Software Integrity	HIGH	32	MEDIUM
Network Components		MEDIUM		Sabotage	MEDIUM	Destruction Equipment: IT Media	MEDIUM	27	MEDIUM
		MEDIUM		Hardware Failures	MEDIUM	Destruction Equipment: IT Media	MEDIUM	27	MEDIUM
Security Utilities		LOW		Software Errors	MEDIUM	Backup/Recovery	HIGH	24	MEDIUM
Buildings		HIGH		Earth Movement	MEDIUM	Departmental Plans	MEDIUM	36	HIGH

Legend

C – Confidentiality. A – Availability. I – Integrity.

T – Threat. V – Vulnerability. A_{Val} – Asset Value. R – Risk.

2.4 Recommendation Phase

Utilizing Table 4, an overall view of the risks can be determined based on need. From the table it can be seen that the most prevalent vulnerability is Software Integrity. This item lies in three separate subgroups which all contain a Very High residual risk score. Based on this, the first item for improvement in the system for the web environment would be for upgrades and training in Information Security in terms of Software Integrity. Preventing Threats from compromising the system will alleviate these threats and reduce the residual risks.

The second most prevalent item comes from the dangers posed from Earth Quakes. Recently Insurance corporations have re-evaluated there risk assessment for a major earthquake along the coast of British Columbia. This re-assessment has produced a major increase in insurance premiums throughout the region. Based on this, the potential for damage to the Buildings, equipment and people is considered High. A policy for back-ups and training to help secure personnel and assets would help this issue.

It is the recommendation of this report that the IT department at the university begins to focus their efforts on creating a secure software infrastructure to prevent hackers, espionage or industrial theft from creating havoc on the web environment.