CASE STUDY : DEVELOP A SECURITY THREAT RISK ASSESSMENT FOR UVIC IT

Braden Simpson
braden@uvic.ca
V00685500

January 24, 2013

1 INTRODUCTION

This report is a consultation for the the University of Victoria IT department, to desribe a method of creating an efficient and effective Security Threat Risk Assessment (STRA). The proposed STRA will go through the following: Preparation Phase, Asset Identification Phase, and the Threat Assessment Phase, and it will cover the university's web environment and services. The UVic web environment has "...many apparent weaknesses in [the] system..."[**?**] The STRA will assess the most valuable assets to secure, and the most important weaknesses to attend to.

2 PREPARATION PHASE

The Preparation phase of the STRA starts off the project, and therefore is crucial to it's success. The following are the deliverables for the Preparation Phase:

- Define roles for all members involved in the STRA - Have succint responsibilities written up and have them assigned early.
- Analyze the current security practices in th place, and any other policies or standards being used.
- Identify current threats and vulnerabilities that have been reported, or current problems that have occurred.
- Identify all stakeholders in the STRA - For example, these could be students, employees, anonymous users visiting the sites, Faculty, IT users, Management, representatives of the university

- Define the goals or objectives of the STRA, and set timeframes.

Once all of this is done, the preparation phase is finished, and the STRA can move into the Asset Identification Phase.

3 Asset Identification Phase

The following table is made to identify the value of certain assets at the University's web environment.

Class	Category	Group	Confid.	Avail Int	Avail op	Integrity
Tangible	Information	Univ IT Dept	High	High	High	High
Tangible	Firmware	Univ IT Dept		Medium	Medium	Medium
Tangible	Facilities	Computer Store		Low	Low	
Tangible	Hardware	Univ IT Dept		Medium	Medium	High
Tangible	Software	Univ IT Dept		Medium	Medium	
Tangible	Facilities	Campus Computers		Medium	Medium	
Intangible	University	Reputation	Low	High	High	High
People	Employees	Univ IT Dept		High	High	
People	Employees	Univ Staff		Medium	Medium	
People	University	Students		Medium	Medium	
People	University	Professors	Medium	Medium	Medium	

The asset values listed in the previous table are a start for the STRA, but when the actual project is underway, the team should investigate further and produce breakdowns for each row listed. One of the most important assets is the university's reputation, which is shown in the table.

4 THREAT ASSESSMENT PHASE

ID No.	Class	Agent	Event	Likelihood	Gravity	Confid.	Avail.	Integrity
31	Deliberate	Individuals	Network Exploitation	Medium	High		High	
32	Deliberate	Individuals	Social Engineering	Medium	Medium	Medium		
40	Deliberate	Groups/Individuals	Delete/Destroy Records	High	Medium			High
41	Deliberate	Groups/Individuals	Corrupt Data	Medium	Medium			Medium
42	Deliberate	Groups/Individuals	Encrypt Files	Medium	Medium		Medium	
43	Deliberate	Groups/Individuals	Misconfigure Software	High	Medium		High	High
44	Deliberate	Groups/Individuals	Misconfigure Hardware	Medium	High		High	
46	Deliberate	Wannabees	DOS Attack	Medium	Medium		Medium	
47	Deliberate	Wannabees	Malicious Code	Low	Medium	Low	Low	Low
48	Deliberate	Wannabees	File Corruption	Medium	Medium			Medium
60	Deliberate	Script Kiddies	Web Defacement	Low	Low			Very Low
94	Deliberate	Hackers	Identity Theft	Medium	High	High		
103	Deliberate	Companies	Patent Infringement	Low	Medium	Low		
106	Deliberate	Individuals	Spam	High	Low	Medium		
108	Deliberate	Individuals	Unauthorized Use	Medium	Medium	Medium	Medium	Medium
118	Accidents	Individuals	Inaccurate Data Input	High	Low			Medium
121	Accidents	Office Staff	Delete Files	High	Low			Medium
122	Accidents	Office Staff	Spill Liquids	Low	Low		Very Low	Very Low
126	Accidents	Cleaning Staff	Unplug Equipment	Medium	Low		Low	
127	Accidents	Individuals	Lose Laptop	High	High	Very High		
129	Accidents	Data Entry Clerks	Data Entry Errors	High	Low			Medium
130	Accidents	Database Admin	Operating Errors	High	Low		Medium	Medium
131	Accidents	Companies	Software Bugs	High	Medium	High		High
132	Accidents	Organizations	Software Integration Errors	High	Medium		High	
133	Accidents	Individuals	Coding Errors	High	Low			Medium
134	Accidents	Individuals	Software Configuration Errors	High	Low		Medium	
135	Accidents	Companies	Design Flaws	High	Medium	High		High
136	Accidents	Companies	Equipment Malfunction	Medium	Medium		Medium	
137	Accidents	Organizations	Installation Errors	Medium	Low		Low	
138	Accidents	Individuals	Hardware Configuration Errors	Medium	Low		Low	
139	Accidents	Individuals	Operator Errors	High	Low		Medium	Medium
147	Accidents	Individuals	Inadvertent Misuse	High	Low		Medium	Medium
156	Accidents	Equipment Operators	Disrupt Production	High	Medium		High	
208	Natural Hazards	Dust	Media Contamination	Low	Low		Very Low	Very Low