University of Victoria, Software Engineering

Security Threat and Risk Assessment Case Study

Jordan Ell
V00660306

January 25, 2013

1 Security Threat and Risk Assessment

This case study focuses on the scenario of the University of Victoria's IT department conducting a security threat and risk assessment review. The University acknowledges that their IT infrastructure has potential security related issues but does not know how to properly handle the situation. This case study will walk through the first three phases of a security threat and risk assessment of the University of Victoria's IT infrastructure. These three steps are: preparation, asset identification, and threat assessment. The end result of this study is not to provide recommendations towards the University, but to lay the frame work for which these recommendations can be based upon.

1.1 Preparation Phase

The preparation phase involves the preparation for assessment of risk inside the University's IT infrastructure. I recommend the following steps be taken in preparation for the assessment to follow.

- Identify stakeholders - Stakeholders may include but are not limited to: students, faculty, professors, IT employees, corporate sponsors, board of directors, student employees, university's reputation, etc ...
- Reviewing current system attacks - Software and hardware attacks are happening constantly around the world. In order to properly combat the attacks being made, you should be up to date on how attackers are successful against other systems and what steps could have been take to avoid the attack or prevent it.

- Reviewing current STRA procedures - Knowing how security threat and risk assessments are being done with other companies or by other contractors allows us to keep the same levels of security standards as the rest of the world.
- Understand the System Being Evaluated - Discover exactly what the University is using for their IT infrastructure. This type of preparation allows the STRA evaluation to know ahead of time where potential leaks in security are more likely to occur as well as avoid unwanted research time for problems that are not present in the tools being used.

With these steps, a STRA evaluator will be well prepared to deal with the problems that the University if facing in regards to their IT infrastructure. Preparation is an important step in the STRA process as it is more than likely to save time and money down the road where larger problems are likely to occur. After these preparations have taken place, time frames and target goals should be set for the later stages of the STRA examination. These steps should define a scope of the project as well as help produce a work plan for future steps.

1.1.1 Asset Identification Phase

The following table is used by the STRA team to identify assets within the Univerisity's IT infrastructure. This table will later be used in the threat assessment phase of the STRA process as outlined in Section 1.1.2.

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

This previous table represents my asset identification phase of the University of Victoria's IT infrastructure. Here I have identified many tangible and people class assets to the university. These assets for the purpose of this case study are very broad and each asset could be further broken down into sub categories for a real STRA evaluation of the IT infrastructure.

1.1.2 Threat Assessment Phase

Finally, the threat assessment of the University's IT infrastructure can be completed here in this section. In the following table, the assets being assessed have been provided for

the purposes of this threat assessment phase. The values in the likelihood, gravity, and one of: confid., avail., or integrity have been filled in for the purposes of this case study.

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

The table created above was created by first entering the likelihood and gravity values based on the provided tables and ruberic in the case study. Next the value of risk was assessed using the likelihood and gravity conversion table provided for the case study.At this point in the STRA process, the table above would now be used to make recommendations to the university's IT Dept staff. However, for the purposes of this case study, we stop here and go no further in the STRA process.