**CIS 481 – Intro to Information Security**

**CLASS EXERCISE # 5**

Grading ID: A7386

**Problem 1**

Complete Exercise 1 from pp. 320 of your text with the following changes. Switch L47’s hardware failure has an expected rate of occurrence of once every 5 years and when that happens it is 100% failure of the device. The SNMP buffer overflow has an expected rate of occurrence of once every five years but only 50% of those attacks are successful. When it is successful, 100% of the asset would be lost or compromised. For server WebSrv6, the invalid Unicode vulnerability is attempted to be exploited once a year but only 10% of those attacks are successful. When those attacks succeed, existing controls keep the loss down to 25% of the asset. For the MGMT45 console, the estimated rate of occurrence of unlogged misuse by the operators is once every 10 years but when it happens, there are no controls in place to reduce the impact, so 100% loss of the asset is likely.

Perform the risk calculations (as shown on p. 287) and determine in what order these vulnerabilities should be addressed based on relative risk. Show your work. (15 pts.)

1st) SwitchL47 (hardware failure) = 22.5

2nd) SwitchL47 SNMP buffer = 11.25

2nd) WebSrv6 = 3

3rd) MGMT45 = 0.55

**Problem 2**

Complete Exercise 3 from p. 320 of your text. You may create a spreadsheet to support your work and paste results into a table here. Be sure to attach spreadsheet, as well, if you choose to use one. (15 pts.)

|  |  |  |  |
| --- | --- | --- | --- |
| **threat category** | **SLE** | **ARO** | **ALE** |
| program mistakes | 5000 | 52 | 260000 |
| Loss of Intellectual property | 75000 | 1 | 75000 |
| software piracy | 500 | 52 | 26000 |
| theft of information (hacker) | 2500 | 4 | 10000 |
| theft of information (employee) | 5000 | 2 | 10000 |
| web defacement | 500 | 12 | 6000 |
| theft of equipment | 5000 | 1 | 5000 |
| virus, worms, trojan horses | 1500 | 52 | 78000 |
| denial of service attack | 2500 | 4 | 10000 |
| earthquake | 250000 | 0.05 | 12500 |
| flood | 250000 | 0.1 | 25000 |
| fire | 500000 | 0.1 | 50000 |

**Problem 3**

Complete Exercise 5 from p. 321 of your text. You may create a spreadsheet to support your work and paste results into a table here. Be sure to attach spreadsheet, as well, if you choose to use one. Be sure to address the questions at the end of the problem. The calculations alone are not sufficient. (20 pts.)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **threat category** | **SLE(post)** | **ARO(post)** | **ALE(post)** | **ACS** | **CBA** | **worth the cost?** |
| program mistakes | 5000 | 12 | 60000 | 20000 | 180000 | yes |
| Loss of Intellectual property | 75000 | 0.5 | 37500 | 15000 | 22500 | yes |
| software piracy | 500 | 12 | 6000 | 30000 | -10000 | no |
| theft of information (hacker) | 2500 | 2 | 5000 | 15000 | -10000 | no |
| theft of information (employee) | 5000 | 1 | 5000 | 15000 | -10000 | no |
| web defacement | 500 | 4 | 2000 | 10000 | -6000 | no |
| theft of equipment | 5000 | 0.5 | 2500 | 15000 | -12500 | no |
| virus, worms, trojan horses | 1500 | 12 | 18000 | 15000 | 45000 | yes |
| denial of service attack | 2500 | 2 | 5000 | 10000 | -5000 | no |
| earthquake | 250000 | 0.05 | 12500 | 5000 | -5000 | no |
| flood | 50000 | 0.1 | 5000 | 10000 | 10000 | yes |
| fire | 100000 | 0.1 | 10000 | 10000 | 30000 | yes |

The controls have changed how often some of these threats occur and the cost per incident. Some controls such as insurance won’t change the frequency of occurrence but will lessen the cost per incident. If the CBA is positive, it is worth the cost of control. However, if the CBA is negative, it is not worth the cost of control.