**CIS-481: Introduction to Information Security**

**In-Class Exercise #5 - Option A**

**IQ Team: 3**

**Names of team members: Noah Smith, Elise Timmons, Samantha Conway, Trevor Rawleigh**

Logistics

A. Get together with other students on your assigned team

B. Discuss and complete the assignment together. Don’t just assign different problems to each teammate as that defeats the purpose of team-based learning.

C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name to denote the number of your assigned team.

**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 points)*

Rr = (Lv x I)(1 – Rc + U)

*Switch L47 Vulnerability 1:*

*(0.2 x 90)(1 – 0 + 0.25) = 22.5*

*Switch L47 Vulnerability 2:*

*(0.1 x 90)(1 – 0 + 0.25 = 11.25*

*WebSrv6 Vulnerability:*

*(0.1 x 100)(1 – 0.75 + 0.2) = 4.5*

*MGMT45 Vulnerability:*

*(0.1 x 5)(1 – 0 + 0.1) = 0.55*

The vulnerabilities should be in the following order, we should always consider the most dangerous risks first.

1. Switch L47 Vulnerability 1
2. Switch L47 Vulnerability 2
3. WebSrv6 Vulnerability
4. MGMT45 Vulnerability

**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 points)*

ARO = Annualized Rate of Occurrence (expected frequency of an attack on a per-year basis)

ALE = Annualized Loss Expectancy (calculated from ARO and SLE [single loss expectancy])

ALE = SLE x ARO

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat Category** | ARO | SLE | ALE |
| Programmer mistakes | 52 | $ 5,000 | $ 260,000 |
| Loss of intellectual property | 1 | $ 75,000 | $ 75,000 |
| Software privacy | 52 | $ 500 | $ 26,000 |
| Theft of information (hacker) | 4 | $ 2,500 | $ 10,000 |
| Theft of information (employee) | 2 | $ 5,000 | $ 10,000 |
| Web defacement | 52 | $ 500 | $ 26,000 |
| Theft of equipment | 1 | $ 5,000 | $ 5,000 |
| Viruses,worms, trojan horses | 52 | $ 1,500 | $ 78,000 |
| DDOS attacks | 4 | $ 2,500 | $ 10,000 |
| Earthquake | 0.05 | $ 250,000 | $ 12,500 |
| Flood | 0.1 | $ 250,000 | $ 25,000 |
| Fire | 0.1 | $ 500,000 | $ 50,000 |

**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 points)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Threat Category** | **SLE** | **ARO** | **ALE** | **CBA** |
| Programmer mistakes | $ 5,000 | 12 | $ 60,000 | $ 180,000 |
| Loss of intellectual property | $ 75,000 | .5 | $ 37,500 | $ 22,500 |
| Software privacy | $ 500 | 12 | $ 6,000 | $ -10,000 |
| Theft of information (hacker) | $ 2,500 | 2 | $ 5,000 | $ -10,000 |
| Theft of information (employee) | $ 5,000 | 1 | $ 5,000 | $ -10,000 |
| Web defacement | $ 500 | 4 | $ 2,000 | $ -6,000 |
| Theft of equipment | $ 5,000 | .5 | $ 2,500 | $ -12,500 |
| Viruses, worms, trojan horses | $ 1,500 | 12 | $ 18,000 | $ 45,000 |
| DDOS attacks | $ 2,500 | 2 | $ 5,000 | $ -5,000 |
| Earthquake | $ 250,000 | .05 | $ 12,500 | $ -5,000 |
| Flood | $ 50,000 | .1 | $ 5,000 | $ 10,000 |
| Fire | $ 100,000 | .1 | $ 10,000 | $ 5,000 |

Some of the values changed in the Cost per Incident and Frequency of Occurrence columns, there are different control methods used for each. The reason some controls could affect some but not the others is because some are less effective.