**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 5**

Names of team members: **Trisia Baltazar, Adrian Boone, Savanah Kennedy, Ryan Smith**

Logistics

A. Get into your regular team

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

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

**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.)

* **Switch L47’s First Risk = (0.2 \* 1) \* (90 \* 1) \* 1.25 = 22.5**
* **Switch L47’s Second Risk = (0.2 \* 0.5) \* (90 \* 1) \* 1.25 = 11.25**
* **WebSrv6’s risk = (1 \* 0.1) \* (100 \* 0.25) \* 1.2 = 3**
* **MGMT45 console’s risk = (0.1 \* 1) \* (5 \* 1) \* 1.1 = 0.55**

**We would go after Switch L47’s First Risk first. Then we would go after Switch L47’s Second Risk. Then we would go after WebSrv6’s risk. Lastly, we would go after MGMT45 console’s risk.**

**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** | **Cost per Incident (SLE)** | **Frequency of Occurrence** | **ARO** | **ALE** |
| Programmer mistakes | 5000 | 1 per week | 52 | 260000 |
| Loss of IP | 75000 | 1 per year | 1 | 75000 |
| Piracy | 500 | 1 per week | 52 | 26000 |
| Hacker | 2500 | 1 per quarter | 4 | 10000 |
| Employee | 5000 | 1 per 6 months | 2 | 10000 |
| Defacement | 500 | 1 per month | 12 | 6000 |
| Theft | 5000 | 1 per year | 1 | 5000 |
| Viruses | 1500 | 1 per week | 52 | 78000 |
| Denial of service | 2500 | 1 per quarter | 4 | 10000 |
| Earthquake | 250000 | 1 per 20 years | 0.05 | 12500 |
| Flood | 250000 | 1 per 10 years | 0.1 | 25000 |
| Fire | 500000 | 1 per 10 years | 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** | **Cost per Incident (SLE)** | **Frequency of Occurrence** | **ARO** | **ALE** | **Control** | **Type** | **CBA** |
| Programmer mistakes | 5000 | 1 per month | 12 | 60000 | 20000 | Training | 180000 |
| Loss of IP | 75000 | 1 per 2 years | 0.5 | 37500 | 15000 | Firewall | 22500 |
| Piracy | 500 | 1 per month | 12 | 6000 | 30000 | Firewall | -10000 |
| Hacker | 2500 | 1 per 6 months | 2 | 5000 | 15000 | Firewall | -10000 |
| Employee | 5000 | 1 per year | 1 | 5000 | 15000 | Physical | -10000 |
| Defacement | 500 | 1 per quarter | 4 | 2000 | 10000 | Firewall | -6000 |
| Theft | 5000 | 1 per 2 years | 0.5 | 2500 | 15000 | Physical | -12500 |
| Viruses | 1500 | 1 per month | 12 | 18000 | 15000 | Antivirus | 45000 |
| Denial of service | 2500 | 1 per 6 months | 2 | 5000 | 10000 | Firewall | -5000 |
| Earthquake | 250000 | 1 per 20 years | 0.05 | 12500 | 5000 | Insurance | -5000 |
| Flood | 50000 | 1 per 10 years | 0.1 | 5000 | 10000 | Insurance | 10000 |
| Fire | 100000 | 1 per 10 years | 0.1 | 10000 | 10000 | Insurance | 30000 |

Some values, such as the cost associated with floods and fires, have changed because the added control (the inclusion of insurance) serves as a mitigating factor keeping the costs associated with those incidents down.

Not all costs are affected by controls in such a way; the theft of intellectual property cannot be made less expensive through the addition of controls in the event that it does happen - only its annualized loss expectancy.

Based on our calculations, we find that for the following threat categories, the proposed controls are **not** worth the cost: software piracy, theft of information (hacker), theft of information (employee), web defacement, theft of equipment, denial-of-service attacks, and earthquakes. For each other threat categories, the proposed controls are worth the cost.