**King Saud University- Ladies Section 333 MIS**

**Management Information Systems Information Security**

**Student Name: Section: Sheet1**

#### 1. If an organization has three information assets to evaluate for risk management as shown in the accompanying data, which vulnerability should be evaluated for additional controls first? Which one should be evaluated last?

An evaluation of the provided asset vulnerabilities results in:

Asset A:

This is a switch that has two vulnerabilities. The first involves a hardware failure likelihood of 0.2 and the second involves a buffer attack likelihood of 0.1. The switch has an impact rating of 90. Assumptions made on this asset have a 75% certainty.

Asset B:

This is a web server that deals with e-commerce transactions. It has one vulnerability with a likelihood of 0.1. However it has an impact rating of 100. Assumptions made on this asset have an 80% certainty.

Asset C:

This is a control console with no password protection with a likelihood of attack of 0.1. It has no controls and an impact rating of 5. Assumptions made on this asset have a 90% certainty.

#### 2. Suppose XYZ Software Company has a new application development project, with projected revenues of $1,200,000. Using the following table, calculate ARO and ALE for each threat category that XYZ Software Company faces for this project.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **XYZ Software Company, major threat categories for new applications development** | **Cost per Incident** | **Frequency of Occurrence** | **SLE** | **ARO** | **ALE** |
| Programmer mistakes | $5,000 | 1 per week |  |  |  |
| Loss of intellectual property | $75,000 | 1 per year |  |  |  |
| Software piracy | $500 | 1 per week |  |  |  |
| Theft of information (hacker) | $2,500 | 1 per quarter |  |  |  |
| Theft of information (employee) | $5,000 | 1 per 6 months |  |  |  |
| Web defacement | $500 | 1 per month |  |  |  |
| Theft of equipment | $5,000 | 1 per year |  |  |  |
| Virus, worms, Trojan horses | $1,500 | 1 per week |  |  |  |
| Denial-of-service attacks | $2,500 | 1 per quarter |  |  |  |
| Earthquake | $250,000 | 1 per 20 years |  |  |  |
| Flood | $250,000 | 1 per 10 years |  |  |  |
| Fire | $500,000 | 1 per 10 years |  |  |  |

#### 3. How might XYZ Software Company arrive at the values in the above table? For each entry, describe the process of determining the cost per incident and frequency of occurrence.

#### 4. Assume a year has passed and XYZ has improved security by applying a number of controls. Using the information from Exercise 2 and the following table, calculate the post-control ARO and ALE for each threat category listed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **XYZ Software Company, major threat categories for new applications development** | **Cost per Incident** | **Frequency of Occurrence** | **Cost of Control** | **ALE** |
| Programmer mistakes | $5,000 | 1 per month | $20,000 | Training |
| Loss of intellectual property | $75,000 | 1 per 2 years | $15,000 | Firewall/IDS |
| Software piracy | $500 | 1 per month | $30,000 | Firewall/IDS |
| Theft of information (hacker) | $2,500 | 1 per 6 months | $15,000 | Firewall/IDS |
| Theft of information (employee) | $5,000 | 1 per year | $15,000 | Physical security |
| Web defacement | $500 | 1 per quarter | $10,000 | Firewall |
| Theft of equipment | $5,000 | 1 per2 years | $15,000 | Physical security |
| Virus, worms, Trojan horses | $1,500 | 1 per6 months | $15,000 | Antivirus |
| Denial-of-service attacks | $2,500 | 1 per quarter | $10,000 | Firewall |
| Earthquake | $250,000 | 1 per 20 years | $5,000 | Insurance/Backups |
| Flood | $50,000 | 1 per 10 years | $10,000 | Insurance/Backups |
| Fire | $100,000 | 1 per 10 years | $10,000 | Insurance/Backups |

**Why have some of the values changed in the columns Cost per Incident and Frequency of Occurrence? How could a control affect one but not the other?**

**Assume the values in the Cost of Control column presented in the table are those unique costs directly associated with protecting against that threat. Calculate CBA for the planned risk control approach for each treat category. For each treat category, determine if proposed control is worth the costs.**

#### Please submit this sheet NEXT CLASS

#### (Saturday section: on 28April2012)

**(Monday Section : on 30April2012)**

**Any delay Will Not Be Accepted**

**Thanks**

**Abeer Bin Humaid**