|  |  |
| --- | --- |
|  | CIS-1290 Principles of Information Security |

Topic 4 Assignment 2

|  |  |
| --- | --- |
| To: | Mike MacDonald |
| From: | Christopher Sigouin |
| Date: | February 21, 2015 |
| Subject: | Complete exercises 3 and 5 |
|  |  |

This assignment is to complete exercises 3 and 5 from chapter 4. Outlined below are both exercises including table formatted data appropriate for their required response. Exercise descriptions are styled in bold and response text color posted in tables is red to improve readability on the page.

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

FORMULAE

ARO = Frequency of Occurrence \* 1 Year

ALE = ARO \* Cost per Incident (SLE)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Category | Cost per Incident (SLE) | Frequency of Occurrences | Prior Annualized Rate of Occurrence  (ARO) | Prior Annualized Loss Expectancy  (ALE) |
| Programmer mistakes | $5,000 | 1 per week | 52 days | $260,000 |
| Loss of intellectual property | $75,000 | 1 per year | 1 day | $75,000 |
| Software piracy | $500 | 1 per week | 52 days | $26,000 |
| Theft of information (hacker) | $2,500 | 1 per quarter  ( 91 days ) | 4 days | $10,000 |
| Theft of information (employee) | $5,000 | 1 per six months | 2 days | $10,000 |
| Web defacement | $500 | 1 per month | 12 days | $6,000 |
| Theft of equipment | $5,000 | 1 per year | 1 day | $5,000 |
| Viruses, worms, Trojan horses | $1,500 | 1 per week | 52 days | $78,000 |
| Denial-of-service attacks | $2,500 | 1 per quarter | 4 days | $10,000 |
| Earthquake | $250,000 | 1 per 20 years  ( 7300 days ) | 0.05 days | $12,500 |
| Flood | $250,000 | 1 per 10 years  ( 3650 days ) | 0.1 days | $25,000 |
| Fire | $500,000 | 1 per 10 years | 0.1 days | $50,000 |

**5. Assume a year has passed and XYZ has improved security by applying a number of controls. Using the information from Exercise 3 and the following table, calculate the post-control ARO and ALE for each threat category listed**.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Threat Category | Cost per Incident | Frequency of Occurrence | Cost of Control | Type of Control | Post-control ARO | Post-control ALE |
| Programmer mistakes | $5,000 | 1 per month | $20,000 | Training | 12 days | $60,000 |
| Loss of intellectual property | $75,000 | 1 per 2 years | $15,000 | Firewall / IDS | 0.5 days | $37,500 |
| Software piracy | $500 | 1 per month | $30,000 | Firewall / IDS | 12 days | $6,000 |
| Theft of information  ( hacker ) | $2,500 | 1 per 6 months | $15,000 | Firewall / IDS | 2 days | $5,000 |
| Theft of information ( employee ) | $5,000 | 1 per year | $15,000 | Physical security | 1 day | $5,000 |
| Web defacement | $500 | 1 per quarter | $10,000 | Firewall | 4 days | $2,000 |
| Theft of equipment | $5,000 | 1 per 2 years | $15,000 | Physical security | 0.5 days | $2,500 |
| Viruses, worms, Trojan horses | $1,500 | 1 per month | $15,000 | Antivirus | 12 days | $18,000 |
| Denial-of-service attacks | $2,500 | 1 per 6 months | $10,000 | Firewall | 2 days | $5,000 |
| Earthquake | $250,000 | 1 per 20 years | $5,000 | Insurance / backups | 0.05 days | $12,500 |
| Flood | $50,000 | 1 per 10 years | $10,000 | Insurance / backups | 0.1 days | $5,000 |
| Fire | $100,000 | 1 per 10 years | $10,000 | Insurance / backups | 0.1 days | $10,000 |

**Why have some values changed in the columns Cost per Incident and Frequency of**

**Occurrence?**

Values have changed in the columns of ‘Cost per Incident’ and ‘Frequency of Occurrence’ because when a control is introduced into the equation it minimizes the ‘Cost per Incident’ and ‘Frequency of Occurrence’. These values are estimated again based on the control being in place. The prior costs and occurrences were based on no controls implemented at all.

**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. In other words, don’t worry about overlapping costs between controls.**

A control could affect one type of threat and not another because of a few factors. It is possible that the nature of the threat cannot be controlled (i.e. Earthquake) and that any controls used to minimize the SLE would have no ability to change it. A natural disaster cannot have its occurrence rate change unless you can control mother nature. But, a control can change the SLE to minimize its damage. As for threat types such as web defacement, a control will change its occurrence rate, but not the SLE because it’s worth is only changeable by the organization who rates it.

**Calculate the CBA for the planned risk control approach for each threat category. For each threat category, determine if the proposed control is worth the costs.**

FORMULAE

CBA = ALE (prior) - ALE (post) – ACS

WORTH? (YES / NO) = ACS < CBA

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Category | CBA | Prior-control  (ALE) | Post-control (ALE) | Cost of Control | Proposed control is worth it? (Yes / No) |
| Programmer mistakes | $180,000 | $260,000 | $60,000 | $20,000 | $20,000 < $180,000  YES |
| Loss of intellectual property | $22,500 | $75,000 | $37,500 | $15,000 | $15,000 < $22,500  YES |
| Software piracy | -$10,000 | $26,000 | $6,000 | $30,000 | $30,000 < -$10,000  NO |
| Theft of information  ( hacker ) | -$10,000 | $10,000 | $5,000 | $15,000 | $15,000 < -$10,000  NO |
| Theft of information  ( employee ) | -$10,000 | $10,000 | $5,000 | $15,000 | $15,000 < -$10,000  NO |
| Web defacement | -$6,000 | $6,000 | $2,000 | $10,000 | $10,000 < -$6,000  NO |
| Theft of equipment | -$12,500 | $5,000 | $2,500 | $15,000 | $15,000 < -$12,500  NO |
| Viruses, worms, Trojan horses | $45,000 | $78,000 | $18,000 | $15,000 | $15,000 < $45,000  YES |
| Denial-of-service attacks | -$5000 | $10,000 | $5,000 | $10,000 | $10,000 < -$5000  NO |
| Earthquake | -$5000 | $12,500 | $12,500 | $5,000 | $5000 < -$5000  NO |
| Flood | $10,000 | $25,000 | $5,000 | $10,000 | $10,000 < $10,000  NO |
| Fire | $30,000 | $50,000 | $10,000 | $10,000 | $10,000 < $30,000  YES |