1) As CIO, you are considering whether to purchase two different security products. You can purchase neither, one or the other, or both. You do not know exactly the number of attacks you will face, but can estimate the you will face a high number of attacks with probability P(high)=0.5, a Medium number of attacks with probability P(Medium)=0.3, and a Low number of attacks with probability P(Low)=0.2. The cost of product 1 is $400,000, and the cost of product 2 is $600,000. The table below gives an estimate of the total losses from attacks for each state of the world for each combination of products purchased.

|  |  |  |  |
| --- | --- | --- | --- |
|  | High | Medium | Low |
| Neither | -2,000,000 | -1,000,000 | -200,000 |
| P1 | -1,000,000 | -400,000 | -100,000 |
| P2 | -600,000 | -300,000 | -100,000 |
| Both | -500,000 | -200,000 | -50,000 |

NOTE: You need to account for both the cost of the products, and the values shown in the table in your analysis.

1. Compute the expected value for each decision and show which decision would be made based on these criteria.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| High | Medium | Low | Cost | EV |
| -2,000,000 | -1,000,000 | -200,000 | 0 | -1,340,000 |
| -1,000,000 | -400,000 | -100,000 | -400,000 | -1,040,000 |
| -600,000 | -300,000 | -100,000 | -600,000 | -1,010,000 |
| -500,000 | -200,000 | -50,000 | -1,000,000 | -1,320,000 |

1. Show which decision would be made based on the maxmin criteria.

Buy P2

1. Write down the regret (opportunity loss) table.

|  |  |  |  |
| --- | --- | --- | --- |
| High | Medium | Low | Cost |
| 1,500,000 | 800,000 | 150,000 | 0 |
| 500,000 | 200,000 | 50,000 | 400,000 |
| 100,000 | 100,000 | 50,000 | 600,000 |
| 0 | 0 | 0 | 1,000,000 |

1. Compute the expected regret for each decision and show which

decision would be made based on these criteria.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| High | Medium | Low | Cost | ER |
| 1,500,000 | 800,000 | 150,000 | 0 | 1,005,000 |
| 500,000 | 200,000 | 50,000 | 400,000 | 715,000 |
| 100,000 | 100,000 | 50,000 | 600,000 | 690,000 |
| 0 | 0 | 0 | 1,000,000 | 1,000,000 |

1. Show which decision would be made based on the minmax criteria.

BUY P2

f. Compute the expected value of perfect information for this problem.

(i.e., how much would you be willing to pay to learn the number of attacks before having to make a decision?).

EVPI = 0.5\*-500,000+0.3\*-200,000+0.2\*-50,000+0 => -320,000

2) You have received a security alert and are considering two possible analysts to assign to investigate the alert. One is inexperienced and has a salary of $25 per hour. The second is more experienced and has a salary of $100 per hour. Both analysts will take around 2 hours to investigate. The inexperienced analyst has a higher error rate of 3% (both false positives and false negatives), while the experienced analyst has an error rate of only 1%. A false positive cost the company $500 in additional investigation time, while a false negative cost the company $50,000 in estimated costs for missing the initial signs of the attack. True positives and negatives both have a cost of 0. Based on prior experience, the probability that the alert corresponds to a real attack is 2%. Compute the expected utility for assigning each analyst to the alert. Which should you choose if you are maximizing expected utility?

Utility = 0.98()+0.02()

3) You are considering two different intrusion detection systems, and want to use the expected value of information to figure out which is a better value for the cost. For each system you scan with the IDS, your prior probability that there is an intrusion is 5%. Your expected cost for a false negative (missing an intrusion) is $25,000. Your expected cost for a false positive (a false alarm) is $500 in time to investigate the alert.

For IDS1, P(Alert|Intrusion) = 0.98, and P(Alert|No Intrusion) = 0.1.

For IDS2, P(Alert|Intrusion) = 0.9, and P(Alert|No Intrusion) = 0.01.

IDS1 costs $500 per system, while IDS2 costs $200 per system.

a) Use Bayes rule to calculate P(Intrusion|Alert) for IDS1.

b) Use Bayes rule to calculate P(Intrusion|Alert) for IDS2.

c) What is the expected value of the information provided by IDS1, compared to missing all of the intrusions?

d) What is the expected value of the information provided by IDS2, compared to missing all of the intrusions?

e) Accounting for all costs, which IDS should you buy?

4) Think of a (simplified) decision problem related to cybersecurity. Write down a description of the decision problem, including the actions you are considering, the possible outcomes, the likelihoods of these outcomes, and the utilities for different outcomes. Draw a decision tree to represent this decision, and apply a relevant method from decision theory to analyze the best decision to make.