Assignment: Risk Management

Professor Deepa Kundur

Please note that this is an *individual* assignment and each person can talk to others, but must ultimately provide their own answers and write their own assignment report.

Questions

1. Suppose an electric power utility (EPU) is actively involved in risk management. The risk identification and assessment phases have resulted in the following information to be used for risk prioritization. Specifically, the EPU has numerous assets with the following identified risks:

- The EPU's corporate data warehouse is susceptible to unauthorized access leading to data deletion and corruption. If compromised, the cost of replacing the information is $1,000,000. The frequency of occurrence of such an attack is estimated to be 0.05 times per year.
- The EPU makes use of a wide area monitoring system (WAMS) whereby a phasor data concentrator owned by the EPU is susceptible to unauthorized access. This can result in data corruption. The data corruption can lead to inefficient decision-making at the control center resulting in an average annual cost of $100,000 to the EPU. The frequency of occurrence of this attack is estimated to be 0.15 times per year.
- Because of a lack of proper access control, it is possible for unauthorized individuals to use dial-in access to remotely access a SCADA supervisory computer. On average, this intrusion would cost $150,000 in damages and recovery and is likely to occur once per year.

An investigation into suitable countermeasures has arrived at the following possibilities:

- To address the risks associated with the corporate data warehouse a new set of firewalls can be purchased and deployed. These firewalls will have an effectiveness of 95%. The total cost of the firewalls is $60,000 and the additional cost of personnel to maintain them is $10,000 per year.
- To address the risks associated with the WAMS phasor data concentrator, access control software may be implemented at a total cost of $5,000. The effectiveness of this solution is estimated to be 100%.
- To address the risks associated with the SCADA system, the dial-in access capability can be eliminated for $1000; here a EPU staff member disables the associated hardware/software. A new method of access to the SCADA supervisory computer is provided through the establishment of a new wireless communication link with appropriate access control for a cost of $10,000. The effectiveness of this solution in preventing intrusions to the SCADA supervisory computer is 75%.

a. Compute the annual loss expectancy (ALE) for each of the risks described above.

b. For each of the risks above, compute the savings in Year 1 of implementing the appropriate countermeasure.

c. From the results of part b, discuss which countermeasures should be implemented and why.

d. Assume that the EPU decides to incorporate all countermeasures (because of legal and compliance restrictions), regardless if whether or not they result in a savings. It is estimated that the countermeasures will take one year to incorporate. What priority should be given to the countermeasures in order to minimize overall possible loss due to attack.

2. Suppose that it is later found that an *additional* intangible cost was missing in the above risk assessment of Question 1. Specifically, unauthorized access to the data warehouse will also result in reputation loss (and subsequent revenue loss) of the EPU as well as privacy disclosure lawsuits. The expected costs resulting from this totals an estimated $2,000,000. How does this change your results to Question 1? Please provide a detailed account with new numerical results.

3. Suppose it is later found that unauthorized access to the SCADA supervisory computer can *additionally* result in injury or even death of EPU field staff in 5% of the cases of unauthorized access. Therefore, the proposed solution of disabling the dial-in access and introducing a new wireless link with appropriate access control is considered to be unsafe since it only results in 75% effectiveness. Safety engineers at the EPU suggest that the minimum effectiveness of an appropriate countermeasure must be 99%. Security engineers at the EPU find a solution that is 99% effective and costs $1,000,000. Risk analysts at the EPU compute that in the event of injury or death of EPU field staff, the overall cost to the EPU (due to unsafe working conditions lawsuits and other intangible costs) totals $3,000,000.

a. Compute the savings of applying this new countermeasure to the SCADA system.

b. Based on your computation in part a, should you implement the countermeasure? Assume there are no other hidden costs than has been stated in this question. Please explain your reasoning in depth and discuss any non-monetary considerations.