IA3600
Homework 1: Risk Prioritization with historical data

Problem
Imagine that you a security analyst consulting for Google ®. You've been asked to consider physical, logical, and human related risks to a data center and decide the best course of action for allocating information security dollars. Google tells you the following about their assets and threats:

The data center serves Google Apps (gmail, video and voice calls, calendars, docs, etc) web services for 10,000 enterprise business consumers in the US. An enterprise consumer (e.g. UNO) pays $5 per user per month to provide Google Apps to their employees. The average enterprise consumer has 100 employees.

When a company signs a contract to use enterprise Google Apps, they are given a service level agreement (SLA) that stipulates that for every 1 minute of downtime Google will deduct 1 dollar per month per user from their bill (down to a minimum of 1$ per month per user). This deduction applies only to the month when downtime occurred.

Based on historical data Google tells you that, on average, when the power goes out, one half (1/2) of the data center goes down for 5 minutes, while the backup generators kick on. Also on average the power goes out once every 2 months.

Also Google employees at the data center fall victim to social engineering or phishing attacks 50 times per year and it costs the data center an average of $1000 each time.

Finally, Google tells you that they provide a 100% data security guarantee to all enterprise customers. For each enterprise user account that is accessed as a result of a Google Data center breach, Google will pay their business customers $100. Based on historical data, Google states that the data center is breached once every 6 years and each breach has an average of 10000 enterprise users that are affected (i.e. their privacy is violated).

Tasks
State the three threats google has given you formally using *Annual Threat Loss Expectancy* (ATLE) and *Expected Threat Impact* (ETI).

Assume you have $10,000 to spend to mitigate risks.

Option 1 buys a second generator to reduce the downtime incurred by power failure by half (i.e. ½ of the data center experiences a 2.5 minute downtime).

Option 2 trains employees to better recognize social engineering an phishing attacks and will reduce incidents by one third (1/3).

Option 3 provides improved network security capabilities it is expected that data center breaches will only occur once every 7 years instead of 6.

How do you allocate your $10,000 and what is your return on investment for each option?
Submit your answers via blackboard in a .doc, .docx, or pdf file.