Vaishnavi Vishwas Pawar
vpawar@iu.edu

Assignment Gordon & Loeb Model

Literature Review (Summary):

The Economic Framework in the Gordon-Loeb model by Lawrence A. Gordon and Loeb Martin P Loeb in the 2002 paper "The Economics of Information Security Investment" play important role in determining if a company will invest more or less in its information security. The level of security must be measured as driven not by the extent to which information is threatened, but by the sum of the cost of protecting vulnerable information and the cost reduction of attacks. This model demonstrates a manner in which organizations can balance their security budgets with performance-enhanced investments that help in the reduction of these factors.

The model reveals how corporations and corporations' protective systems risk information sets. It is perhaps surprising that it is not, in most cases, advantageous for firms to invest in safeguarding especially fragile categories of organization's data and the data asset's work security. The argument is founded on the premise that the more authenticity is at stake, the more involved it is to protect it at any cost. Instead, the model claims that the concern of securing the intermediate levels of vulnerability is more beneficial as the cost of doing so is minimal when compared with the marginal benefit acquired in the process. This can be illustrated as, when the vulnerability level increases, the effort to reduce vulnerability cost is also increasing at a decreasing rate, which in turn leads to a phenomenon of limited returns in the highly vulnerable risk cases.

There is a significant aspect of the Gordon-Loeb model that states that the appropriate investment in information security is usually less than 37% of the estimated financial loss. The approach shows the tendency of many organizations to spend too much on protecting information. It shifts the focus towards aspiring to increase the surplus of security investments over costs, leading to a more systematic and deliberate spending on cybersecurity. Whereby threats are managed and funds distributed in a prudent manner, making the possible risks and the funds efficient.

Key Assumptions of the Gordon-Loeb Model:

1. Vulnerability and Potential Loss: The model assumes that each information set contains a vulnerability (v), which represents the likelihood of a successful breach. The financial impact of a breach is known as the potential loss (λ). Security investments aim to reduce, but not completely eliminate, this vulnerability.
2. Decreasing Returns on Security Investments: Investments in information security reduce vulnerability but yield diminishing returns. This means that every additional dollar spent on security becomes less effective at reducing vulnerability, making it critical for businesses to determine the optimal level of investment.

3. Fixed Threat Probability: While security investments can reduce vulnerability, the probability of a threat (t) does not change. Firms have no control over or reduction in the likelihood of threats occurring, only the chance that these threats will be successful.
4. Focus on Expected Loss, not Maximum Loss: Instead of focusing on the worst-case scenario, the model encourages firms to calculate investments based on the expected loss ($L = t * \lambda$). This approach helps businesses avoid overspending by making decisions based on the likelihood of a breach rather than the potential loss.
5. Risk-Neutral Firms: The model assumes that firms are risk-neutral, which means they are unconcerned about risk variation and focus their security investments solely on maximizing expected returns. This avoids the assumption that businesses are overly cautious or risk averse.
6. Midrange Vulnerability Focus: One of the key takeaways is that protecting midrange vulnerabilities is frequently more cost effective. The model demonstrates that securing highly vulnerable or very low-risk information can be inefficient due to high costs or low returns on investment, respectively.

Key Findings of the Gordon-Loeb Model:

1. Optimal Investment Cap (37% of Expected Loss): The model determines that the optimal security investment is less than 37% of the expected loss from a security breach. Spending above this limit results in diminishing returns and is not economically justified.
2. Midrange vulnerabilities provide the best ROI: The most cost-effective security investments target information with medium-level vulnerabilities. These areas provide the highest return on investment (ROI), balancing vulnerability reduction with reasonable costs.
3. Marginal Returns Decrease with Investment: As businesses invest more in security, the marginal return on each additional dollar falls. This emphasizes the importance of optimizing investments rather than simply increasing security spending.
4. Not always optimal to protect highly vulnerable sets: Protecting extremely sensitive information can become prohibitively expensive. According to the model, firms are often better off securing midrange vulnerabilities, which provide a higher return on investment.
5. Security Overinvestment is Common: Many businesses overinvest in security by focusing too heavily on high-risk scenarios without considering the cost-effectiveness of their investments. The model enables managers to allocate resources more strategically, reducing waste.

Vaishnavi Vishwas Pawar
vpawar@iu.edu

Analysis: Impact of Uncertainty in Vulnerability on Optimal Security Investment

When uncertainty enters the vulnerability component of the Gordon-Loeb model, it complicates how businesses allocate their security budgets. Firms have traditionally known their vulnerability and can invest accordingly, but when vulnerability is uncertain, spending becomes more cautious. Firms may be hesitant to make large investments if they are unsure whether they will significantly reduce risks, for fear of misallocating resources due to an overestimation or underestimation of the threat.

From my point of view, uncertainty frequently leads to more conservative security spending. In an uncertain environment, companies may choose to spread their investments across multiple assets rather than overcommitting to protect a single vulnerable area. The reasoning is straightforward: when vulnerability is not clearly defined, the return on security investment is uncertain, making firms hesitant to risk large sums without a clear benefit.

For example, consider a company that deals with two systems: one with obvious vulnerabilities and ambiguous vulnerabilities. The company may invest more in the system with known risks because the potential return on that investment is more predictable. In contrast, a system with uncertain vulnerabilities may choose to invest less or take a wait-and-see approach, making incremental improvements rather than committing a large sum up front.

On the other hand, firms may increase their security spending if they see uncertainty as a greater threat. This is less common. In most cases, uncertainty drives companies to spend more cautiously, incrementally, focusing on resource optimization to balance cost and risk rather than aggressively investing.

Tasks to Perform:

1. Modify the Python code to change the slope m and intercept c to alter the placement of the cost of the investment line.

The Python code was modified to change the slope m and intercept c of the cost line. The slope was set to m = 0.1, while the intercept was set to c = 0.02. These values were chosen to generate a cost line that gradually increases and begins with a low initial cost. This allowed us to simulate a scenario in which security investments begin low and gradually increase.

Explanation for Changing m, c:

Slope of the Cost Line (m)

- I chose m = 0.1 to ensure that the cost of investment increased gradually, allowing for a broader range of investment values before the cost outweighed the benefit.

Vaishnavi Vishwas Pawar
vpawar@iu.edu

- A lower slope was chosen to simulate a scenario in which security costs rise gradually, giving you more freedom in terms of how much you can invest while still reaping benefits.
- Alternatively, if m had been set higher (for example, m = 0.2 or m = 0.25), the cost line would have risen more steeply, reducing the number of investments that provide a significant benefit. This would result in an earlier intersection of cost and benefit, lowering the optimal investment point.

Intercept of the Cost Line (c)

- I set c = 0.02 to create a low initial cost. This was done to simulate a scenario in which some basic security investment is required even at the lowest levels of investment.
- Keeping c low ensures that the cost line does not start too high while also allowing the model to optimize investments with a gradual increase in cost.
- If c had been set higher (for example, c = 0.05), the cost line would begin at a higher point, indicating a larger initial investment cost. This would further narrow the range of optimal investments, as the benefits would have to outweigh the costs much sooner.

2. Change the value of V (Vulnerability) and observe the change in the EBIS curve.

- I experimented with v = 0.95 and 0.8:
    - v = 0.95: Because this high vulnerability reflects a system that is prone to risks, the EBIS curve rises sharply, indicating that investing in security can yield significant benefits.
    - v = 0.8: This slightly lower vulnerability corresponds to a more moderate-risk system. The EBIS curve remains steep but slightly flatter than with v = 0.95, indicating that there is still a need for investment but not as aggressively.
- The value of v determines how quickly the EBIS curve rises. The higher the vulnerability, the greater the potential return on investment in security.
- The choice between v = 0.95 and v = 0.8 represents a balance between aggressive security spending and risk tolerance.
    - A higher vulnerability value, such as v = 0.95, indicates that the system is highly vulnerable, and firms are more likely to invest aggressively to protect against potential breaches.
    - On the other hand, v = 0.8 represents a system with moderate vulnerability, which may still require significant investment but allows for a more balanced approach.
- Firms dealing with critical systems or sensitive data may prefer the v = 0.95 configuration due to the high risk of a security breach, whereas firms dealing with less critical systems may choose v = 0.8 to avoid over-investment while still mitigating risks.
- In both cases, the EBIS curve demonstrated that investing in security yielded significant returns, but the higher vulnerability (v = 0.95) resulted in a steeper curve, indicating more aggressive investment.

Vaishnavi Vishwas Pawar
vpawar@iu.edu

3. Determine the optimal placement where the difference between expected benefit and cost of investment is maximized.

The Python code was used to find the optimal investment point, which maximizes the difference between the EBIS curve and the cost line. In both cases (v = 0.95 and v = 0.8), the optimal investment was determined to be z = 1.00, implying that the maximum investment provided the greatest benefit.

This result implies that, in both scenarios, it is advantageous to invest as much as possible in security due to the slow-rising cost line and the significant return on investment.

How I Calculated the Optimal Placement:

- The optimal placement was calculated by determining the investment level at which the difference between the EBIS curve and the cost line is greatest. This point represents the investment level at which you get the most value for your money in terms of security.
- To accomplish this, the code computes the difference between the EBIS values and the cost values for each possible investment level (z), using the following equation:
    - Difference = EBIS (z) – Cost (z).
    - Difference=EBIS(z)−Cost(z)
- The Python function np.argmax() was used to find the index with the greatest difference, which is the best investment opportunity.

How The Python Code Works:

- First, the code generates a set of possible investment levels (z) ranging from 0 to 1.
- It calculates the EBIS curve using the current value of v (vulnerability), which influences how quickly the benefit of investment grows.
- It then calculates the cost line using the slope (m) and intercept values (c).
- Then it identifies the investment level at which the difference between the EBIS curve and the cost line is greatest.
- Finally, it identifies this point on the graph as the optimal investment point and displays the EBIS and cost values for that point.

Why is the optimal placement at z = 1.00

- The optimal investment was discovered to be at z = 1.00 in both the v = 0.95 and v = 0.8 cases. This means that the highest possible investment yields the greatest benefit.
- This is due to the fact that the EBIS curve (particularly in areas of high vulnerability) continues to rise significantly, whereas the cost line increases slowly. As a result, it is prudent to invest as much as possible in security, particularly in highly vulnerable systems.

Vaishnavi Vishwas Pawar
vpawar@iu.edu

The following is the Python code to calculate the optimal investment, and the changes made to get the graph (visualization).

vaishnavi_ GordonModel.ipynb ☆

File Edit View Insert Runtime Tools Help All changes saved

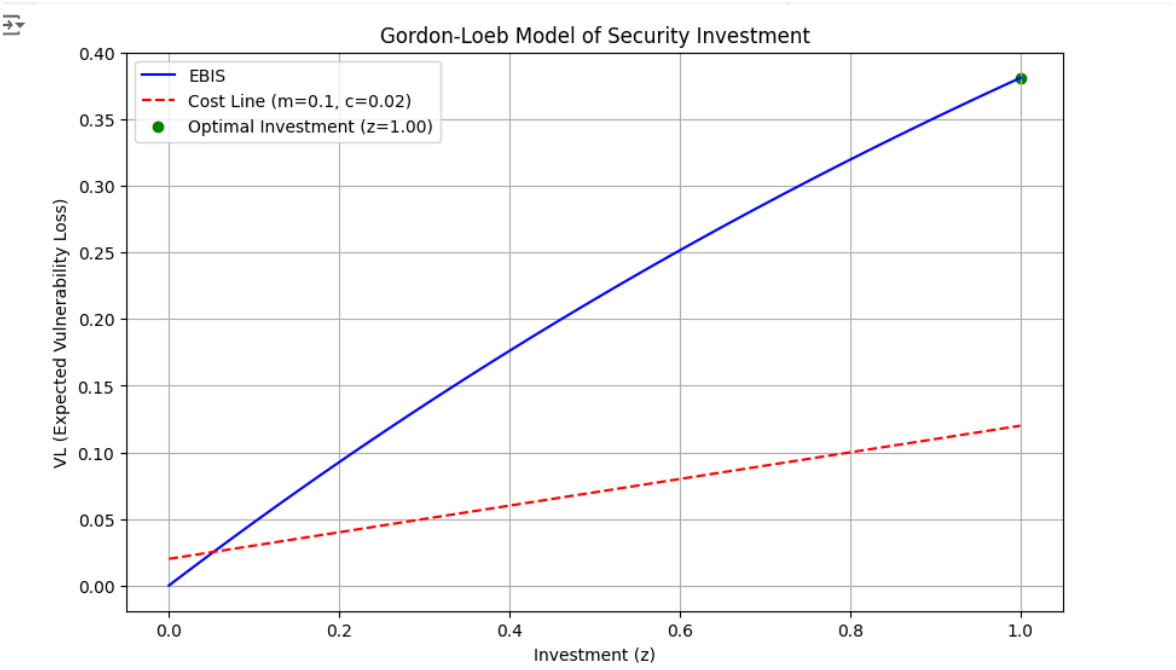
+ Code + Text

```python
import numpy as np
import matplotlib.pyplot as plt

alpha = 10
v = 0.95    # vulnerability, adjust the value to see change in the EBIS curve. Remember 0<=V<=1
L = 1      # potential loss in case of a breach

# Define S(z, v) - security breach probability after investment z
def S(z, v):
    return v ** (alpha * z + 1)

# list of investment values
z_values = np.linspace(0, 1, 100)

# Calculate EBIS (Expected Benefit from Info Sec) for each investment value
EBIS_values = [(v - S(z, v)) * L for z in z_values]

# Plotting
plt.figure(figsize=(10, 6))

# Plot the EBIS curve
plt.plot(z_values, EBIS_values, label='EBIS', color='blue')

#To change the cost of investment line's position and angle change the values of m and c i.e. the slope and y-intercept respectively.
# Adjust the slope (m) and y-intercept (c)
m = 0.1 # Slope of the line; adjust as needed. A value < 1 makes it less steep.
c = 0.02  # Y-intercept

# Calculate the cost of investment line
cal_cost = [m * z + c for z in z_values]

# Find the maximum difference between EBIS and cost of investment
diff_val = np.array(EBIS_values) - np.array(cal_cost)
optimalIdx = np.argmax(diff_val)
OptimalInvestment = z_values[optimalIdx]

# Plot the cost of investment with the given slope and intercept
plt.plot(z_values, m * z_values + c, label=f'Cost Line (m={m}, c={c})', linestyle='--', color='red')
```

```python
# Mark the optimal point on the graph
plt.scatter(OptimalInvestment, EBIS_values[optimalIdx], color='green', label=f'Optimal Investment (z={OptimalInvestment:.2f})')

# Additional settings
plt.title('Gordon-Loeb Model of Security Investment')
plt.xlabel('Investment (z)')
plt.ylabel('VL (Expected Vulnerability Loss)')
plt.legend()
plt.grid(True)

# Show the plot
plt.show()

# Print the optimal investment point, EBIS value, and cost at the optimal point
print(f"Optimal Investment: {OptimalInvestment:.2f}")
print(f"EBIS at Optimal Investment: {EBIS_values[optimalIdx]:.4f}")
print(f"Cost at Optimal Investment: {cal_cost[optimalIdx]:.4f}")
```

Python code modified

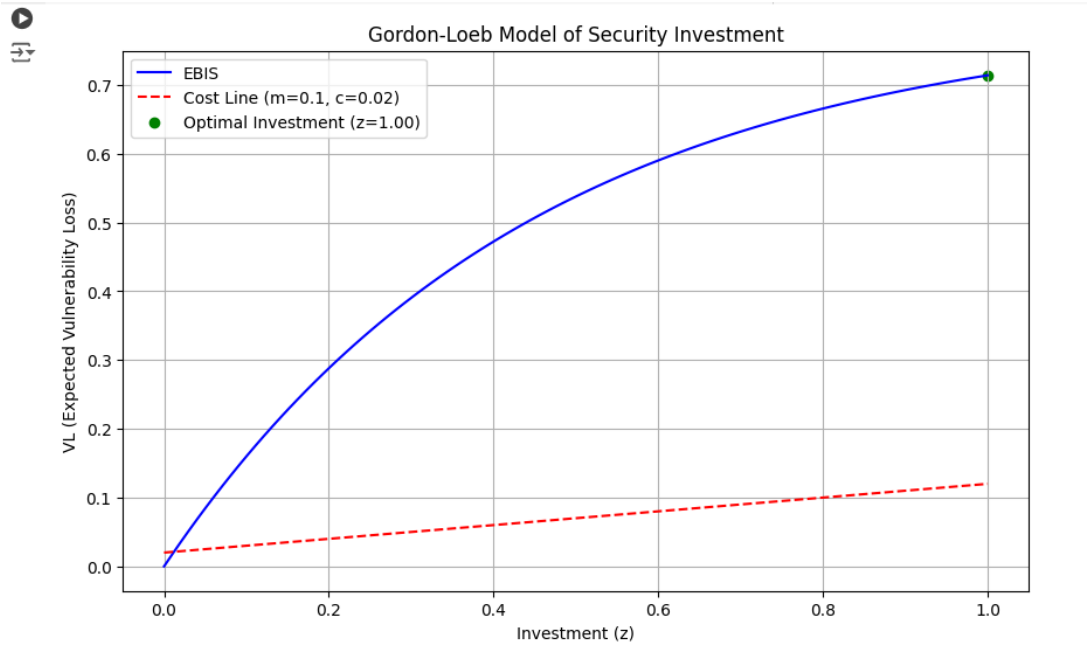
Vaishnavi Vishwas Pawar
vpawar@iu.edu




```
Optimal Investment: 1.00
EBIS at Optimal Investment: 0.3812
Cost at Optimal Investment: 0.1200
```

Output: Optimal Investment = 1, when v = 0.95, c = 0.02 and m = 0.1

To better explain my above points, I have included a visualization when v = 0.8, c = 0.02, and m = 0.1.




```
Optimal Investment: 1.00
EBIS at Optimal Investment: 0.7141
Cost at Optimal Investment: 0.1200
```

Output: Optimal Investment = 1, when v = 0.8, c = 0.02 and m = 0.1

Vaishnavi Vishwas Pawar
vpawar@iu.edu

Conclusions and Implications of My Findings:

1. Maximum investment is optimal: In both cases (v = 0.95 and v = 0.8), the optimal investment point was z = 1.00, implying that investing the maximum amount provided the greatest benefit. This suggests that significant investment in risk mitigation is required for highly vulnerable systems.
2. Vulnerability Matters: The v = 0.95 configuration produced a steeper EBIS curve, indicating that more aggressive investment is required when a system is highly vulnerable. On the other hand, v = 0.8 indicated a more moderate investment strategy while still favoring maximum investment.
    - *Clarification on Spending Strategy:* It is important to note that while uncertainty in vulnerability often leads to more conservative spending, as businesses prefer to spread resources and reduce risk when threats are ambiguous, the situation changes when the vulnerability is clearly defined.
    - Firms with known high vulnerability, such as v = 0.95, are more likely to pursue an aggressive investment strategy because they have a better understanding of the potential risks and benefits of mitigation. This justifies increased security spending, which is reflected in the optimal investment results.
3. Cost Control: The slow-rising cost line (due to m = 0.1 and c = 0.02) enabled a wide range of investments to be made without incurring rapidly increasing costs. This emphasizes the importance of weighing vulnerability against cost when deciding on security investments.
4. Practical Implication: For highly vulnerable systems, it is critical to devote as much budget as possible to security, as the potential benefits outweigh the costs. However, if the vulnerability is moderate, significant investment is still required, but there may be less urgency to maximize spending.