Security Investment Models

Tyler Moore

CSE 5/7338
Computer Science & Engineering Department, SMU, Dallas, TX

Lectures 7&8

Review of security investment so far

- Metrics for quantifying security benefits
  - \( ALE_0 \): expected loss without security investment
  - \( ALE_s \): expected loss with security investment
  - \( EBIS_s = ALE_0 - ALE_s \)
  - \( ENBIS_s = ALE_0 - ALE_s - c \)

- High-level investment metrics
  - ROSI
  - NPV
  - IRR

NPV and IRR visualized

Security investment questions worth answering

Q: Should we invest in security?
A: Yes, if \( ENBIS_s > 0 \)

Q: Should we invest in defense A or B?
A: Choose the one with higher ROSI (or NPV if considering longer time horizons)

Q: How much should we invest?
A: The Gordon-Loeb model can help offer an answer
Gordon-Loeb model

- Model investment decision over a single period
- Use Bernoulli loss assumption (suffer loss $\lambda$ with fixed probability $p_s$)
- The probability of loss depends on two factors: security level and the system’s inherent vulnerability
- The breach probability function maps these factors to probabilities
- Gordon and Loeb’s model use assumptions about security investment to derive optimal investment levels based on the breach probability functions

Breach probability function

\[ S : \mathbb{R}^+ \times [0, 1] \to [0, 1] \]

Maps a security investment $c$ and an exogenous vulnerability $v \in [0, 1]$ to the probability $p$ of incurring a loss of size $\lambda$. Furthermore:

- An invulnerable organization ($v = 0$) is exposed to no risk regardless of its security investment: $p = S(c, 0) = 0$ for all $c$
- Vulnerability determines the probability of loss of an organization which does not invest in security: $p = S(0, v) = v$ for all $v$
- $S$ is continuous and twice-differentiable

Breach probability functions

\[
S'(c, v) = \frac{v}{(\alpha c + 1)^{\beta + 1}}
\]

\[
S''(c, v) = \frac{\beta v^{\beta + 1}}{(\alpha c + 1)^{\beta + 2}}
\]

- $\alpha > 0$ and $\beta > 1$ capture security productivity
- Measure how efficiently the security investment reduces probability of loss
- Can think of $\alpha \in [0, 1]$ as coefficient for linear model relating $c$ to security level $s$ (i.e., $s = \alpha \cdot c$)
Visualizing $S(c, v)$ for $\alpha = 1$

$$S(c, v) = \frac{v}{(vc + 1)^{\beta}}$$

Back to last week’s benefit metrics

$$\text{EBIS} = \lambda (v - S(c, v))$$

$$\text{ENBIS} = \lambda (v - S(c, v)) - c$$

The Gordon-Loeb model assumes that for all $v \in [0, 1]$, and all $c > 0$, $S$ is strictly convex in $c$, i.e.,

$$\delta_c S(c, v) < 0 \quad \text{and} \quad \delta_{cc} S(c, v) > 0$$

(Note: $\delta_c$ is the first partial derivative with respect to $c$, and $\delta_{cc}$ is the second partial derivative with respect to $c$.)

Decreasing marginal returns to security investment

Why is it reasonable to model security investment with decreasing marginal returns?

- In the Gordon-Loeb model, decreasing marginal returns emerge from convexity assumption about $S$
- Why is this defensible?
  - **Benefits to security are often concave** – a rational defender implements the measures with best cost-benefit ratio first, leaving less efficient alternatives if the security budget increases
  - **Costs to security are often convex** – combining defenses can be more expensive than deploying just one (compatibility issues, management complexity)
- Empirical validation (or refutation) of this assumption is an open research question
Choosing an optimal security investment

- Given a range of security investment levels, how can a manager choose the optimal amount?
- If security investment adheres to diminishing marginal returns, then we can identify the investment level $c^*$ that maximizes the expected net benefit $\text{ENBIS}$

Choosing an optimal security investment

Informally, we look for the investment level where the marginal benefit of security is equal to its marginal cost

Formally, we seek the cost level $c^*$ where:

$$c^* = \max_c \text{ENBIS}(c)$$

We find $c^*$ using the first-order condition (FOC):

$$\delta_c \text{EBIS}(c^*) = 1$$

We find $c^*$ using the first-order condition (FOC):

$$\delta_c \text{EBIS}(c^*) = 1$$

For $c^* > 0$, this condition maximizes $\text{ENBIS}$ because $\text{EBIS}$ is concave.

Choosing an optimal security investment, visualized

![Graph showing the relationship between security investment and expected net benefit](image-url)
Gordon-Loeb model
Baseline investment models
Information security risk management
Measuring the security level

Breach probability function
Decreasing marginal returns
Optimal security investment

The Gordon-Loeb model is very sensitive to values assigned to $v$: small differences can lead to very different optimal investment levels.

Furthermore, $v$ can be hard to estimate in practice.

So they came up with a rule of thumb: never spend more than 37% of your expected loss on security.

Definition

(Gordon–Loeb Rule): The optimal security investment $c^*$ is bounded from above by $\lambda/e$, where $e$ is the base of the natural logarithm.

Linear breach probability function

Let’s start with the simplest possible model.

We use the Bernoulli loss assumption.

Two outcomes \((0, \lambda)\)

\[(0 : 1 - p_s, \lambda : p_s)\]

We assume security investment is effective.

\[c = \lambda s\]

For unit loss $\lambda = 1$:

\[c = s\]

We can even use a linear breach probability function

\[S(s, v) = v \cdot (1 - s) \quad \text{for} \quad s \in [0, 1].\]

One final simplification

We reduce the action space to just two possibilities – secure ($s = 0$) and insecure ($s = 1$)

<table>
<thead>
<tr>
<th>State</th>
<th>Security $s = c/\lambda$</th>
<th>Probability of loss $p$</th>
<th>Expected loss $E(\lambda)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insecure</td>
<td>0</td>
<td>$v$</td>
<td>$\lambda v$</td>
</tr>
<tr>
<td>Secure</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

What are the trade-offs between using a linear breach probability function and the one used in the Gordon-Loeb model?
Exponential breach probability function

- If diminishing marginal returns is important to include in the model, and we want to retain the Bernoulli loss assumption, then the breach probability function should be convex.
- But the complexity of Gordon-Loeb’s function
  \[ S(c, v) = \frac{v^\alpha}{c^{\alpha+1}} \]
  can be hard to justify.
- We can use a simpler model with one variable for tuning the security productivity instead of two:
  \[ S(s, v) = v^\beta - s \]
- We require \( \beta > 1 \), and also require \( S(s, 0) = 0 \) for all \( s \) and \( S(0, v) = v \), as in the Gordon-Loeb model.

Exponential breach probability function, visualized

Optimal security investment

We can compute the optimal security investment \( s^* \) using the first-order condition of the ENBIS

\[
\delta_s(\text{ENBIS}(s^*)) = 0
\]
\[
\delta_s(v - S(s, v) - s) = 0
\]
\[
\delta_s(v - v^\beta - s) = 0
\]

which has an analytical solution for \( v > 0 \):

\[
s = \frac{\log(v\log(\beta))}{\log(\beta)}
\]

Why is this a reasonable first-order condition? Why does it lead to optimal investment?
Another way to maximize benefit

\[ \delta_s(\text{EBIS}(s^*)) = 1 \]

which is equivalent to

\[ \delta_s(\text{ENBIS}(s^*)) = 0 \]

Why? Substitute \( \text{ENBIS}(s^*) = \text{EBIS}(s^*) - s^* \)

\[ \begin{align*}
\delta_s(\text{EBIS}(s^*) - s^*) &= 0 \\
\delta_s(\text{EBIS}(s^*)) - \delta_s(s^*) &= 0 \\
\delta_s(\text{EBIS}(s^*)) - 1 &= 0 \\
\delta_s(\text{EBIS}(s^*)) &= 1
\end{align*} \]

One more caveat

- Some values of \( \beta \) will be negative for the investment condition
- In particular, \( s^* < 0 \) for \( \beta \in (1, e^{1/v}) \)
- Consequently, we set the optimal security level as follows:

\[ s^* = \max \left\{ \log \left( \frac{\log(\beta)}{\log(\beta)} \right), 0 \right\} \]

- If \( \beta \in (1, e^{1/v}) \), we say that the organization is indefensible
- The security investment must become more productive to justify any investment

How optimal investment varies

- Let’s first review how to make the plot for the linear breach probability function
- Then let’s explore how optimal investment varies for the exponential breach probability
- Today’s code: \( \text{http://lyle.smu.edu/~tylerm/courses/econsec/code/secinv3.R} \)
Information security risk management

Just as it can be useful to translate infosec risks and defenses into the language of investment (ROSI, NPV, etc.), one must also be aware of terminology from risk management. As IT becomes essential to many businesses, the border between information security investment and general risk management has blurred.

Risk management terminology overview

Risk analysis
- identification
- quantification

Risk management
- acceptance
- mitigation
- avoidance
- transfer

Risk monitoring
- validation
- documentation

Cyberinsurance

Risk acceptance

After risks are identified and quantified, they must be "managed."

The simplest option is to do nothing.

Such "risk acceptance" is prudent when:
1. Worst-case loss is small enough to be paid from proceeds or reserves.
2. Probability of occurrence is smaller than other business risks that threaten the organization’s survival.

This is why the security policies for start-ups are often weaker than for entrenched firms.

Risk mitigation

If risk is too big and probable to be accepted, risk mitigation aims to reduce the probability and severity of a loss.

This is where security investment comes in.

Recall that the optimal level of investment normally leaves residual risk that must be dealt with using acceptance, avoidance, or transfer.
Risk avoidance

- Aims to reduce the probability and severity of loss, as in risk mitigation
- However, rather than use technology, here one forgoes risky activities
- This introduces opportunity costs of lost business opportunities
- Example: online merchant refusing overseas orders due to high fraud risk
- Example: company disconnects database with customers' personal information online
- Question: what are the opportunity costs in these cases?

Risk transfer

- The final option is to buy an insurance contract to recover any future losses incurred
- This is only available in limited circumstances
- Why has the cyber-insurance market remained small?
  - Difficulty in quantifying losses
  - Even when possible, many firms would rather keep quiet than share with an insurance company
  - Externalities mean that the costs of insecurity are often borne by others
  - Correlated risk is prevalent

Risk management example: credit card issuers

Credit card issuers regularly manage fraud

1. Risk acceptance: fraud is paid from the payment fees charged to merchants
2. Risk mitigation: install anti-fraud technology (raises costs of security)
3. Risk avoidance: downgrade high-risk cardholders to debit or require online verification (leads to lost business)
4. Risk transfer: structure consumer credit risk and sell it on the market

Measuring the security level

- The security investment models we've discussed directly map security costs onto benefits
- However, it can be more accurately thought of as a two-step mapping
  - Security is mapped to a security level
    - Deterministic
    - Defined by available technology
  - Security level is mapped to benefit
    - Probabilistic (depends on attacker behavior)
    - Defined by firm's risk exposure
Security production function as 2-step mapping

To validate a direct mapping from cost to benefit, one must find many companies choosing among the same sets of technologies AND with similar risk profiles.

Using two-step mapping, we can directly measure how cost relates to security level, usually without regard to the risk facing a firm.

We still need measurements mapping from the security level to benefits, which can still be hard to find.

Security indicators measure the security level

How can we measure the security level? Unlike cost and benefit, which are directly measured in monetary terms, the security level is latent. Consequently, we need indirect measures of the security level.

**Definition**

A security indicator is an observable signal conveying information about the security level.