Managing security investment

Overview

Motivation

- It can be important to frame information security decisions using the language of business

  ⇒ Security investment decisions must balance expected costs and benefits

  - To model rational decisions, we start by simplifying our assumptions of attacker behavior
    - Strategic adversary
      - Attacker exogenously given, follows a probability of attack known to the defender
      - In this sense, we treat security like a safety problem
    - When is the simplified attacker model appropriate?
      - Indiscriminate attackers (e.g., phishing, scanning)
      - Targeted attackers (e.g., spear-phishing, adaptive attacks)

Security cost and benefits

<table>
<thead>
<tr>
<th>cost of security</th>
<th>benefit of security</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>$</td>
</tr>
<tr>
<td>direct / indirect</td>
<td>expected prevented losses</td>
</tr>
<tr>
<td>variable / fixed</td>
<td>$</td>
</tr>
<tr>
<td>onetime / recurring</td>
<td>$</td>
</tr>
<tr>
<td>sunk / recoverable</td>
<td>$</td>
</tr>
</tbody>
</table>

Notes
Cost of security

Definition (Cost of security, security level) The cost of security $c$ is the amount spent to reach a security level $s$. No security investment \( (c = 0) \) implies $s = 0$, and for any $c > 0$, $s$ increases monotonically in $c$.

Definition (Effective security investment) If security investment is effective, the security level can be approximated by the cost of security, i.e., $s \approx c$.

When does the effective security investment definition apply? When not?

Security benefit: reduction of losses incurred in the absence of security

- In other words: take a small fixed loss now to reduce the chances of a large but uncertain future loss
- We already have the tools to deal with uncertainty about outcomes: expected utility!

Expected utility (discrete)

$$E[U(a)] = \sum_{o \in O} U(o) \cdot P(o|a)$$

Expected utility (continuous)

$$E[U(a)] = \int_{u}^{v} U(x) \cdot P(x|a) dx$$
**Loss distribution function**

**Definition**

(Loss distribution function) Let $L_s : \mathbb{R}^+ \rightarrow [0, 1]$ be the family of probability distribution functions describing the monetary losses incurred from insecurity for a given security level $s$.

- $L_0$ is the loss distribution function in the absence of security investment
- Benefit of security: $L_s - L_0$
- We use expected utility to compare outcomes for the loss functions

**Comparing loss functions (discrete)**

$$E[U(L)] = \sum_{o \in O} U(o) \cdot L(o)$$

**Annual loss expectancy**

**Definition**

(ALE) The annual loss expectancy $A{LE}_s$ is the expected loss per period due to information security failures given security level $s$,

$$A{LE}_s = E(L_s) = \int_0^{\infty} x \cdot L_s(x) \, dx .$$

Note that annual suggests a multi-period view. Even when this isn’t the case, the ALE term is used.

**Annual loss expectancy visualized**

$$A{LE}_s = E(L_s) = \int_0^{\infty} x \cdot L_s(x) \, dx \quad A{LE}_0 = E(L_0) = \int_0^{\infty} x \cdot L_0(x) \, dx$$
Definition

(EBIS) The expected benefit of information security $EBIS_s$ is the difference between the loss expectancy without security and the loss expectancy given security level $s$,

$$EBIS_s = ALE_0 - ALE_s = E(L_0) - E(L_s) = \int_0^\infty x \cdot (L_0(x) - L_s(x)) \, dx.$$ 

Definition

(ENBIS) The expected net benefit of information security investment $ENBIS_s$ is given by the expected benefit of information security minus the cost of the investment to reach security level $s$.

$$ENBIS_s = EBIS_s - c = ALE_0 - ALE_s - c,$$

or, assuming effective security investment,

$$ENBIS_s = EBIS_s - s.$$

Straightforward investment rule: only invest if $ENBIS_s > 0$

Let’s calculate the metrics for discrete loss functions

<table>
<thead>
<tr>
<th>Loss</th>
<th>$L_0$</th>
<th>$L_s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>0.8</td>
<td>0.9</td>
</tr>
</tbody>
</table>

- $ALE_0 = 0 \cdot 0.8 + 2000 \cdot 0.2 = $400
- $ALE_s = 0 \cdot 0.9 + 2000 \cdot 0.1 = $200
- $EBIS_s = ALE_0 - ALE_s = $400 - $200 = $200
- $ENBIS_s = ALE_0 - ALE_s - c = $200 - $c$

Bernoulli loss assumption

- OK, so continuous loss distribution functions are nice, but they can be difficult to analyze
- Not to mention it can be hard to justify assumptions about how the loss distribution might be shaped
- Simplified scenario
  - Two loss outcomes: $\{0, \lambda\}$
  - $\lambda > 0$: fixed loss, occurs with $p_s = L_s(\lambda)$
  - With probability $1 - p_s = L_s(0)$, suffers no loss
Recall the antivirus example

- Suffering a hack costs $2000, AV costs $75
- Without AV, 10% chance of being hacked
- With AV, 1% chance of being hacked

<table>
<thead>
<tr>
<th>Action</th>
<th>E(\text{no hack})</th>
<th>E(\text{hack})</th>
<th>E(\text{\text{$2000}})</th>
<th>\text{$75}</th>
<th>\text{$2000}</th>
</tr>
</thead>
<tbody>
<tr>
<td>buy AV</td>
<td>\text{$75}</td>
<td>0.99</td>
<td>\text{$75}</td>
<td>0.01</td>
<td>\text{$95}</td>
</tr>
<tr>
<td>don't buy AV</td>
<td>0.9</td>
<td>0.01</td>
<td>\text{$2000}</td>
<td>0.1</td>
<td>\text{$200}</td>
</tr>
</tbody>
</table>

Notes

Metrics under Bernoulli loss assumption

\[ \text{ALE}_s = (p_s \cdot \lambda + (1 - p_s) \cdot 0) = p_s \cdot \lambda \]
\[ \text{EBIS}_s = \frac{(p_0 \cdot \lambda + (1 - p_0) \cdot 0) - (p_s \cdot \lambda + (1 - p_s) \cdot 0)}{E(L_s)} = \frac{(p_0 - p_s) \cdot \lambda}{E(L_s)} \]
\[ \text{ENBIS}_s = \frac{(p_0 \cdot \lambda + (1 - p_0) \cdot 0) - (p_s \cdot \lambda + (1 - p_s) \cdot 0) - s}{E(L_s)} = \frac{(p_0 - p_s) \cdot \lambda - s}{E(L_s)} \]

Notes

Metrics under Bernoulli loss assumption & $\lambda = 1$

Things get simplified even more if we scale the loss to 1 ($\lambda = 1$)

\[ \text{ALE}_s = p_s, \]
\[ \text{EBIS}_s = (p_0 - p_s), \quad \text{and} \]
\[ \text{ENBIS}_s = p_0 - p_s - s \]
Return on security investment (ROSI)

Definition
(ROSI) The return on information security investment ROSI is the ratio of the expected net benefit over the cost of security,

\[
\text{ROSI} = \frac{\text{ENBS}}{\text{c}} = \frac{A\text{LE}_0 - A\text{LE}_s - c}{c}
\]

NPV: evaluating security investments over time

Definition
(NPV) The net present value NPV aggregates the expected net benefit of information security over multiple future periods into a monetary equivalent at present,

\[
\text{NPV} = -c_0 + \sum_{t=1}^{\infty} \frac{A\text{LE}_t - A\text{LE}_s - c_t}{(1 + r)^t}
\]

where
- \(c_0\) is the one-off cost of security at \(t = 0\),
- \(c_t\) are recurring costs of security in period \(t\) (if any),
- \(A\text{LE}_t\) is loss expectancy for period \(t\) and security level \(s\), and
- \(r\) is the discount rate.

Internal rate of return

Definition
(IRR) The internal rate of return IRR is the discount rate \(r^*\) at which a decision maker using NPV as a sole criterion is indifferent between making the security investment or not, i.e., \(\text{NPV} = 0\).
**Security metrics**

**High-level investment metrics**

**Example: countering data breaches**

Comparing two security investments to combat data loss

<table>
<thead>
<tr>
<th>Variable</th>
<th>Security investment option 1</th>
<th>Security investment option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data loss prevention</td>
<td>User training</td>
</tr>
<tr>
<td></td>
<td>Est.</td>
<td>Est.</td>
</tr>
<tr>
<td>Initial investment</td>
<td>15 K</td>
<td>6 K</td>
</tr>
<tr>
<td>License and deployment</td>
<td></td>
<td>Training material</td>
</tr>
<tr>
<td>Maintenance, opportunity cost</td>
<td>1 K</td>
<td>3 K</td>
</tr>
<tr>
<td>of false positives</td>
<td></td>
<td>Fee and lost work time</td>
</tr>
<tr>
<td>w/o security investment</td>
<td>5 K</td>
<td>20 K legal settlement, probability 25%</td>
</tr>
<tr>
<td>with security investment</td>
<td>2 K</td>
<td>False negatives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 K</td>
</tr>
<tr>
<td>Residual risk (lapses etc.)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Exercise: compute $ENBIS_s$ for both options

Which approach (DLP or training) appears to be the better investment over 10 years using expected-net benefit calculations over 10 years?

$$ENBIS_s = t_{max} \cdot (ALE_0 - ALE_s - c_t) - c_0$$

DLP: $ENBIS_s(1) = \ ?$

User training: $ENBIS_s(2) = \ ?$

These calculations favor DLP, but what about the net-present value?

**Net-present value**

$$NPV_s = -c_0 + \sum_{t=1}^{t_{max}} \frac{ALE_0.t - ALE_s.t - c_t}{(1+r)^t}$$

Let’s calculate NPV assuming $r = 5\%$, $t_{max} = 10$

$$NPV_s(1) = -15K + \sum_{t=1}^{10} \frac{5K - 2K - 1K}{(1.05)^t} = \$443$$

$$NPV_s(2) = -6K + \sum_{t=1}^{10} \frac{5K - 1K - 3K}{(1.05)^t} = \$1,722$$

Using NPV, we find training to be better value than DLP!
Internal rate of return

Rather than assume a rate of return for a comparable investment, we can find the “break-even” rate of return, i.e., choose \( r \) where \( NPV_s = 0 \).

\[
NPV_s = -c_0 + \sum_{t=1}^{T} \frac{ALE_{0,t} - ALE_{s,t} - c_t}{(1 + r)^t}
\]

\[
NPV_s(1) = -15K + \sum_{t=1}^{10} \frac{5K - 2K - 1K}{(1 + r)^t} \quad \Rightarrow r = 5.6\%
\]

\[
NPV_s(2) = -6K + \sum_{t=1}^{10} \frac{5K - 1K - 3K}{(1 + r)^t} \quad \Rightarrow r = 10.5\%
\]

User training still a good investment even if you must borrow money at 10% interest rate.

NPV and IRR visualized

Option 1: Data loss prevention

Option 2: User training

R

- R is an open-source statistical programming language
- Supports script-based programming
- Supported by vibrant community, extensive libraries support nearly anything you’d want to do with statistics
- We will use it later on for data exploration and analysis when studying e-crime
- However I introduce it today for two reasons
  - To give you a tool to make calculations that would be tedious by hand (e.g., NPV)
  - To lessen the learning curve when we use it more extensively later on

Download R from [http://www.r-project.org/](http://www.r-project.org/)

- Official tutorial: [http://cran.r-project.org/doc/manuals/R-intro.html](http://cran.r-project.org/doc/manuals/R-intro.html)
- I prefer Zuur’s Beginner’s Guide to R, available for free download to SMU students at [http://dx.doi.org/10.1007/978-0-387-93837-0](http://dx.doi.org/10.1007/978-0-387-93837-0)
- Can also download PDFs of all chapters from [http://lyle.smu.edu/~tylerm/courses/econsec/rbegin.html](http://lyle.smu.edu/~tylerm/courses/econsec/rbegin.html) using course username/password
- Chapters 2 and 5 (for plots) are good starting points
- To get help with a function, type `?functionName` at the interpreter
- If you don’t know the name, type `??anytext` to do a text-search on all help files
Exploring models and metrics with R

Interactive R demo

Download code from
http://lyle.smu.edu/~tylerm/courses/econsec/code/r-intro.R

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

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

Lawrence Gordon

Martin Loeb
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**

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

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

\( \alpha > 0 \) 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 \( S^I(c,v) \) for \( \alpha = 1 \)**

\[
S^I(c,v) = \frac{v}{(c + 1)^\beta}
\]
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 $c$.)

### 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):

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

For \( c^* > 0 \), this condition maximizes ENBIS because EBIS is concave.

Choosing an optimal security investment, visualized

Gordon-Loeb Rule

- 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.
Let’s start with the simplest possible model

1. We use the Bernoulli loss assumption

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

   \( \{0 : 1 - p_s, \lambda : p_s\} \)

2. We assume security investment is effective

   \( c = \lambda s \)

   For unit loss \( \lambda = 1 \):

   \( c = s \)

3. We can even use a linear breach probability function

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

One final simplification

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

<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?

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 \( S(c, v) = \frac{v}{(\alpha c + 1)^\beta} \) 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
Optimal security investment

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

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

which has an analytical solution for $v > 0$:

$$s = \log \left( \frac{\log(v \log(\beta))}{\log(\beta)} \right)$$

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 $\text{ENBIS}(s^*) = \text{EBIS}(s^*) - s^*$

$$\delta_s(\text{EBIS}(s^*) - s^*) = 0$$
$$\delta_s(\text{EBIS}(s^*)) - \delta_s(s^*) = 0$$
$$\delta_s(\text{EBIS}(s^*)) - 1 = 0$$
$$\delta_s(\text{EBIS}(s^*)) = 1$$
One more caveat

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

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

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

How optimal investment varies

![Security Investment Example](image.png)

Investment models in R

- 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.
- Screencast: [https://www.youtube.com/watch?v=t9g5u75g3G0](https://www.youtube.com/watch?v=t9g5u75g3G0)
- Before you review those links, let’s see what you can do in class as an exercise.

Linear breach probability function

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

- Task 1: write a function called `bpf` in R implementing the linear breach probability function.
- Task 2: plot the graph for $\nu = 1$ (hint: use a sequence of x values between 0 and 1).
- Task 3: add plots for $\nu = 1/2$ and $1/4$ (hint: use the `lines` command, vary line type using `lty` parameter).
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

2-step mapping makes measurement easier

- 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

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