(Part I: Economics of Security)
Lecture 2: Security Investment Analysis

Dusko Pavlovic

Outline

Cost-Benefit Analysis for Security Investment

Tasks of CIO
Accounting

Security Risk Analysis
Level of Security Investment

Security has a major economic impact
Security has a major economic impact

Conclusions

- It is hard to measure security risk
- Security industry has an incentive to
  - overstate and oversimplify the risk
  - offer "one size fits all" solutions
- The organisations must
  1. assess their own risks
  2. evaluate the costs and the benefits of security
  3. make decisions about their security investment
Further problem

... But

- even if we know risks, costs and benefits of security,
- how should we make rational security decisions?

Plan

1. Given the costs and benefits of security, decide how much to invest in it.
2. Given the risks, derive the costs and benefits.

Assumption

ToySec company has assessed

- its security risks and their costs
- the potential benefits of security protections

The outcome of the assessment is given in a table

<table>
<thead>
<tr>
<th>time</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>security benefit</td>
<td>$B_0$, $B_1$, $B_2$, ...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>security cost</td>
<td>$C_0$, $C_1$, $C_2$, ...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Accounting of security investments

Question

Given the costs and the benefits, how do we calculate the value of security investments?

Example 1

- On January 1, 2012, ToySec buys a firewall for £200,000.
- During the year 2012, ToySec accumulates
  - firewall operating costs of £100,000, and
  - security benefits of £400,000
Basic accounting: Value

Net cash flow (NCF)

2012-01-01 - £200K
2013-01-01 - £400K - £100K = £300K

Value (V) = total cash flow

2012-01-01 - £200K
2013-01-01 - £200K + £300K = £100K

Example 1

On January 1, 2013, ToySec buys a firewall for £200,000.
During the year 2013, ToySec is expected to accumulate
- firewall operating costs of £100,000, and
- security benefits of £400,000

Example 1 again

- security benefit: £400,000
- security cost: £200,000
- security profit: £200,000
- security benefit: 150%

annual return on investment = investment profit / investment cost
Concept 1: Annual return on investment (AROI)

**Definition**

Annual return on investment (AROI) is the accounting concept obtained by dividing:

- Investment profit in a given year, obtained by subtracting:
  - the costs \( C_1 \) from
  - the benefits \( B_1 \)
  with
- Investment costs \( C_0 \), needed to generate the profit.

\[
\text{AROI} = \frac{B_1 - C_1}{C_0}
\]

**Decision rule**

- AROI > 100% — accept the investment
- AROI < 100% — reject the investment
- AROI = 100% — offers no grounds for a decision

---

**Example 1 yet again**

<table>
<thead>
<tr>
<th>time</th>
<th>1-1-2012</th>
<th>1-1-2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>security benefit</td>
<td>0</td>
<td>£400,000</td>
</tr>
<tr>
<td>security cost</td>
<td>£200,000</td>
<td>£100,000</td>
</tr>
</tbody>
</table>

\[
\text{AROI} = \frac{400,000 - 100,000}{200,000} = 150\%
\]

\[\Rightarrow \text{invest!}\]

---

**Example 2**

<table>
<thead>
<tr>
<th>time</th>
<th>1-1-2012</th>
<th>1-1-2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>security benefit</td>
<td>0</td>
<td>£300,000</td>
</tr>
<tr>
<td>security cost</td>
<td>£250,000</td>
<td>£100,000</td>
</tr>
</tbody>
</table>

\[
\text{AROI} = \frac{300,000 - 100,000}{25,000} = 80\%
\]

\[\Rightarrow \text{do not invest!}\]

---

**Example 3**

<table>
<thead>
<tr>
<th>time</th>
<th>1-1-2012</th>
<th>1-1-2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>security benefit</td>
<td>0</td>
<td>£300,000</td>
</tr>
<tr>
<td>security cost</td>
<td>£200,000</td>
<td>£100,000</td>
</tr>
</tbody>
</table>

\[
\text{AROI} = \frac{300,000 - 100,000}{200,000} = 100\%
\]

\[\Rightarrow \text{use a different accounting concept?}\]
Accounting of security investments

Question

How do we calculate return on multi-period investments?

Example 4

- On January 1, 2013, ToySec buys an intrusion detection system for £200,000.
- During the year 2013 ToySec is expected to accumulate
  - firewall operating costs of £100,000, and
  - security benefits of £400,000

Example 4

<table>
<thead>
<tr>
<th>time</th>
<th>1-1-2013</th>
<th>1-1-2014</th>
<th>1-1-2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>security benefit</td>
<td>0</td>
<td>£400,000</td>
<td>£450,000</td>
</tr>
<tr>
<td>security cost</td>
<td>£200,000</td>
<td>£100,000</td>
<td>£100,000</td>
</tr>
</tbody>
</table>

Simple return on investment (SROI)

**Definition**

Simple return on investment (SROI) is the accounting concept obtained by dividing

- total investment profit in a given period, obtained by subtracting
  - total costs \( \sum C_i \) from
  - total benefits \( \sum B_i \)
  - with
  - total costs \( \sum C_i \) needed to generate the profit
Concept 1: Simple return on investment (SROI)

**Definition**
Simple return on investment (SROI) is the accounting concept obtained by dividing:
- total investment profit in a given period, obtained by subtracting:
  - total costs \( \sum C_i \) from
  - total benefits \( \sum B_i \)
with
- total costs \( \sum C_i \), needed to generate the profit

\[
SROI = \frac{\sum B_i - \sum C_i}{\sum C_i}
\]

**Decision rule**
The more the better

---

**Accounting of security investments**

**Question**
What is the net present value of multi-period investments?

**Example 4 again**
- On January 1, 2013, ToySec buys an intrusion detection system for £200,000.
- During the year 2013 ToySec is expected to accumulate:
  - firewall operating costs of £100,000, and
  - security benefits of £400,000
- During the year 2014 ToySec is expected to accumulate:
  - firewall operating costs of £100,000, and
  - security benefits of £450,000
- ToySec's cost of capital is 15%.
Concept 2: Net Present Value (NPV)

**Definition**
The net present value (NPV) of an investment is the sum of:
- the annual values of the investment, obtained by subtracting for each year $t$:
  - the costs $C_t$ from
  - the benefits $B_t$
- discounted by the annual cost of capital $k$ which is the minimal rate of return that every project needs to earn in order for the organization to break even.

$$\text{NPV} = \sum_{t=0}^{n} \frac{B_t - C_t}{(1 + k)^t}$$
where usually $B_0 = 0$, except when there are instant benefits.

**Decision rule**
- $\text{NPV} > 0$ — accept the investment
- $\text{NPV} < 0$ — reject the investment
- $\text{NPV} = 0$ — offers no grounds for a decision

**Example 4**

<table>
<thead>
<tr>
<th>time</th>
<th>1-1-2013</th>
<th>1-1-2014</th>
<th>1-1-2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>security benefit</td>
<td>0</td>
<td>£400,000</td>
<td>£450,000</td>
</tr>
<tr>
<td>security cost</td>
<td>£200,000</td>
<td>£100,000</td>
<td>£100,000</td>
</tr>
<tr>
<td>cost of capital</td>
<td>15%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$$\text{NPV} = -200,000 + \frac{300,000}{1.15} + \frac{350,000}{1.15^2}$$
$$= -200,000 + 260,870 + 264,650$$
$$= 325,520$$

$\Rightarrow$ invest!

**Example 5**

<table>
<thead>
<tr>
<th>time</th>
<th>1-1-2013</th>
<th>1-1-2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>security benefit</td>
<td>0</td>
<td>£400,000</td>
</tr>
<tr>
<td>security cost</td>
<td>£280,000</td>
<td>£100,000</td>
</tr>
<tr>
<td>cost of capital</td>
<td>15%</td>
<td></td>
</tr>
</tbody>
</table>

$$\text{NPV} = -280,000 + \frac{300,000}{1.15}$$
$$= -280,000 + 260,870$$
$$= -19,130$$

$\Rightarrow$ do not invest!
Example 6

<table>
<thead>
<tr>
<th>time</th>
<th>1-1-2013</th>
<th>1-1-2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>security benefit</td>
<td>0</td>
<td>£400,000</td>
</tr>
<tr>
<td>security cost</td>
<td>£200,000</td>
<td>£100,000</td>
</tr>
<tr>
<td>cost of capital</td>
<td>50%</td>
<td></td>
</tr>
</tbody>
</table>

\[
\text{NPV} = -200,000 + \frac{300,000}{1.5} \\
= -200,000 + 200,000 \\
= 0
\]

⇒ take risk aversion into account?

Accounting of security investments

Question

Is it better to invest in security or in something else?

Concept 3: Internal rate of return (IRR)

Definition

The internal rate of return (IRR) of an investment is the discount rate which makes the net present value of a security investment equal to 0.

\[
0 = \sum_{t=0}^{n} \frac{B_t - C_t}{(1 + \text{IRR})^t}
\]

where usually \(B_0 = 0\), except when there are instant benefits.

Example 7

- On January 1, 2013, ToySec buys an intrusion detection system for £280,000.
- During the years 2014 and 2015 ToySec is expected to accumulate
  - firewall operating costs of £100,000, and
  - security benefits of £400,000
- ToySec’s cost of capital is 15%.

Concept 3: Internal rate of return (IRR)

Decision rule

Suppose that an investment \(A\) has a rate of return \(k_A\).

\[
\begin{align*}
\text{IRR} > k_A & \quad \text{— invest in security (not in } A) \\
\text{IRR} < k_A & \quad \text{— do not invest in security (invest in } A) \\
\text{IRR} = k_A & \quad \text{— consider other preferences}
\end{align*}
\]
### Example 7

<table>
<thead>
<tr>
<th>time</th>
<th>1-1-2013</th>
<th>1-1-2014</th>
<th>1-1-2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>security benefit</td>
<td>0</td>
<td>£400,000</td>
<td>£400,000</td>
</tr>
<tr>
<td>security cost</td>
<td>£280,000</td>
<td>£100,000</td>
<td>£100,000</td>
</tr>
<tr>
<td>rate of return of A</td>
<td>15%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[
0 = -280,000 + \frac{300,000}{1 + \text{IRR}} + \frac{300,000}{(1 + \text{IRR})^2}
\]

\[
\text{IRR} = 70.12\% > 15\% = k_A
\]

\[
\Rightarrow \text{invest in security!}
\]

### Example 8

<table>
<thead>
<tr>
<th>time</th>
<th>1-1-2013</th>
<th>1-1-2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>security benefit</td>
<td>0</td>
<td>£400,000</td>
</tr>
<tr>
<td>security cost</td>
<td>£280,000</td>
<td>£100,000</td>
</tr>
<tr>
<td>cost of capital</td>
<td>15%</td>
<td></td>
</tr>
</tbody>
</table>

\[
0 = -280,000 + \frac{300,000}{1 + \text{IRR}} + \frac{300,000}{(1 + \text{IRR})^2}
\]

\[
\text{IRR} = 7.14\% < 15\% = k_A
\]

\[
\Rightarrow \text{invest in } A
\]

### How do we evaluate benefits of security?

**Primary security benefits** are the value of the losses prevented by the security measures.

**Secondary security benefits** are the value of the gains in reputation and reliability incurred from security.

### Outline

- **Cost-Benefit Analysis for Security Investment**
  - **Security Risk Analysis**
    - **Security benefit**
    - Evaluating risk
      - Random variable
      - Expected value
      - Variance
      - Risk aversion
  - Level of Security Investment

### How do we evaluate benefits of security?

**Components**

- negative part: risk decrease
  - the expected value of prevented losses
- positive part: utility
  - the expected value of gains

\[
B = U + R
\]
Utility of reputation and reliability

Initial assumption of accounting
All utility and demand functions are given.

Evaluating risk

Actuarial science
- the main tool of the insurers
- applied probability theory
- we need the basic actuarial calculations

Example 1

Problem: Prediction
You live in an orchard and pick an apple every day. What is the risk that the apple that you will pick today has a worm in it?

Data
- You cannot tell whether an apple has a worm by looking at it.
- You have recorded your tasting experience from last 30 days, and you found that
  - 18 apples were tasty,
  - 8 apples had a worm,
  - 4 apples were unripe.

Solution: Probability
Denote the quality of the apple that you will pick by $Q$. Then

$$\Pr(Q = \text{tasty}) = \frac{18}{30}$$
$$\Pr(Q = \text{wormed}) = \frac{8}{30}$$
$$\Pr(Q = \text{unripe}) = \frac{4}{30}$$
Example 1
Formalization: Random variable
- The qualities of the available apples are viewed as a function $Q : \text{Apples} \rightarrow \text{Tastes}$

$Q$ induces a probability distribution $Pr(Q=?)$:

- $Pr(Q=\text{tasty}) = \frac{|\{a \in \text{Apples} | a \text{ tasty}\}|}{30} \approx 0.6$ (unripe)
- $Pr(Q=\text{wormed}) = \frac{|\{a \in \text{Apples} | a \text{ wormed}\}|}{30} \approx 0.27$ (tasty)
- $Pr(Q=\text{unripe}) = \frac{|\{a \in \text{Apples} | a \text{ unripe}\}|}{30} \approx 0.13$ (wormed)

Random variable

Definition
A random variable is a function $X : A \rightarrow V$

which induces a probability distribution

$Pr(X=? : V \rightarrow [0,1])$ where

$Pr(X = v) = \frac{|\{a \in A | X(a) = v\}|}{\#A}$

Example 2
Problem: Quantifying risk
- You sell apples for 50¢ each.
- When an unripe apple is returned, you have to replace it by another apple for free.
- When an apple with a worm is returned, you have to replace it by another apple for free, and return 50¢.

What is your risk in this business?
Example 2

Problem: Quantifying risk

- You sell apples for 50¢ each.
- When an unripe apple is returned, you have to replace it by another apple for free.
- When an apple with a worm is returned, you have to replace it by another apple for free, and return 50¢.

How much do you expect to lose?

Example 2

Data

<table>
<thead>
<tr>
<th>apple quality</th>
<th>tasty</th>
<th>wormed</th>
<th>unripe</th>
</tr>
</thead>
<tbody>
<tr>
<td>loss</td>
<td>0 c</td>
<td>100 c</td>
<td>50 c</td>
</tr>
<tr>
<td>probability</td>
<td>1/3</td>
<td>1/3</td>
<td>1/3</td>
</tr>
</tbody>
</table>

Solution: Expected value of the loss

expected loss per apple = \( \frac{18}{30} \cdot 0 + \frac{8}{30} \cdot 100 + \frac{4}{30} \cdot 50 = 33.3 \)

Example 2

Formalization: Expected value

- The random variable \( L : \text{Apples} \rightarrow \mathbb{R} \) is distributed as follows:
  \[ \Pr(L = 0) = \frac{18}{30}, \quad \Pr(L = 100) = \frac{8}{30}, \quad \Pr(L = 50) = \frac{4}{30}, \quad \Pr(L = \text{other}) = 0 \]

- The expected value of the random variable \( L \) is
  \( \int_{\text{Apples}} L = \sum_{r \in \text{R}} r \cdot \Pr(L = r) \)
  \( = 100 \cdot \frac{8}{30} + 50 \cdot \frac{4}{30} = 33.3 \)

Expected value

Definition

The expected value of a random variable \( X : A \rightarrow \mathbb{R} \) is

\[ \int_A X = \sum_{x \in A} X(x) \cdot \Pr(x) \]
Expected value

Proposition
The expected value of a random variable $X : A \rightarrow \mathbb{R}$ can equivalently be computed as

$$\int_A X = \sum_{r \in \mathbb{R}} r \cdot \Pr(X = r)$$

What is risk?

Definition
Risk is the expected (i.e. average) value of the loss.

Remark
The price of an insurance policy is the value of the insured risk increased by insurer's profit.

Example 3

Problem: Quantifying the IT risk

Type of incident:
- denial of service (DoS)
- loss of data (LD)
- loss of IP (LIP)

Losses:
- £1M
- £2M
- £3M

Example 3

Data: ToySec Admin. Dept. A

<table>
<thead>
<tr>
<th>Incident</th>
<th>DoS</th>
<th>LD</th>
<th>LIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>£1M</td>
<td>£2M</td>
<td>£3M</td>
</tr>
<tr>
<td>Probability</td>
<td>0.06</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Example 3
Data: ToySec Admin. Dept. A

<table>
<thead>
<tr>
<th>incident</th>
<th>DoS</th>
<th>LD</th>
<th>LIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>cost</td>
<td>1M</td>
<td>2M</td>
<td>3M</td>
</tr>
<tr>
<td>probability</td>
<td>0</td>
<td>.06</td>
<td>0</td>
</tr>
</tbody>
</table>

Risk: Expected loss

\[ \int \text{loss}_A = .06 \cdot 2,000,000 = 120,000 \]

Example 4
Data: ToySec Design Dept. D

<table>
<thead>
<tr>
<th>incident</th>
<th>DoS</th>
<th>LD</th>
<th>LIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>cost</td>
<td>1M</td>
<td>2M</td>
<td>3M</td>
</tr>
<tr>
<td>probability</td>
<td>0</td>
<td>0</td>
<td>.04</td>
</tr>
</tbody>
</table>

Risk: Expected loss

\[ \int \text{loss}_D = .04 \cdot 3,000,000 = 120,000 \]

Example 4
Data: ToySec Sales Dept. S

<table>
<thead>
<tr>
<th>incident</th>
<th>DoS</th>
<th>LD</th>
<th>LIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>cost</td>
<td>1M</td>
<td>2M</td>
<td>3M</td>
</tr>
<tr>
<td>probability</td>
<td>.06</td>
<td>.015</td>
<td>.01</td>
</tr>
</tbody>
</table>

Risk: Expected loss

\[ \int \text{loss}_S = .06 \cdot 1,000,000 + .015 \cdot 2,000,000 + .01 \cdot 3,000,000 = 120,000 \]

Comparison

Question

- Are all three companies at the same risk?

Comparison

Overview

<table>
<thead>
<tr>
<th>incident</th>
<th>DoS</th>
<th>LD</th>
<th>LIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>cost</td>
<td>1M</td>
<td>2M</td>
<td>3M</td>
</tr>
<tr>
<td>probability</td>
<td>0</td>
<td>.06</td>
<td>0</td>
</tr>
</tbody>
</table>

Observations

- D and S may lose 3M
- S’s total loss probability is .085
- ...
Question

▶ Is the average (expected value of) loss a good measure of risk?
▶ How far does \( \int X \) deviate from \( \int X \)?

Deviation

Definition

The absolute deviation of a random variable \( X : A \rightarrow \mathbb{R} \) is

\[
\sigma(X) = \int_{x \in A} |X - \int_{x \in A} X|
\]

Exercise

Compute absolute deviation for the following random variables:

▶ the value of unbiased 6-sided die
▶ the number of heads coming up when 3 unbiased coins are flipped

Standard deviation

Definition

The standard deviation of a random variable \( X : A \rightarrow \mathbb{R} \) is

\[
\sigma(X) = \sqrt{\int_{x \in A} (X - \int_{x \in A} X)^2}
\]
Standard deviation

**Exercise**

Compute the standard deviation for the following random variables:

- the value of unbiased 6-sided die
- the number of heads coming up when 3 unbiased coins are flipped

**Comparison of the deviations**

**Remark**

If the random variable X is expressed using a unit of measure (e.g.,), then its expected value, as well as its deviation, is expressed in the same unit of measure.

Variance

**Definition**

The variance of a random variable \( X : A \rightarrow \mathbb{R} \) is the square of its standard deviation:

\[
\text{Var}(X) = \int_{A} \left( X - \int_{A} X \right)^2 \, d\mu
\]

**Exercise**

Compute the variance, the standard deviation, and the absolute deviation of the respective risks of the administrative, the design and the sales departments of ToySec Corp.

**Conclusion**

**Lemma**

\( \alpha, \sigma \) and \( \text{Var} \) induce the same order on random variables:

\[
\alpha(X) \leq \alpha(Y) \\
0 \leq \sigma(X) \leq \sigma(Y) \\
\text{Var}(X) \leq \text{Var}(Y)
\]

**Conclusion**

Absolute deviation, standard deviation and variance

- measure how well a random variable fits its expected value
- \( \sigma \) and \( \text{Var} \) are correspond to normally distributed (Gaussian) deviations and have a simpler statistic than \( \alpha \)
- \( \sigma(X) \) and \( \alpha(X) \) are the same units as \( X \), whereas \( \text{Var}(X) \) is in the square units
Risk aversion

Example

You are given 3 choices:

A: a prefect die is thrown, and you get 60 if it falls on 6; otherwise 0;
B: an unbiased coin is flipped, and you get 20 if it the head falls up; otherwise 0;
C: you get 10 for sure.

What would you choose?

Risk aversion informally

Intuition

You are

risk-seeking if your preference order is $A > B > C$
risk-averse if your preference order is $C > B > A$
risk-neutral if you are indifferent between the three gambles, i.e. $A \sim B \sim C$

Preference

Definition

A preference over a set $S$ is a binary relation $\succ$ on $S$ such that for all $X, Y, Z \in S$ holds

\[ X \succ Y \land Y \succ Z \implies X \succ Z \]
\[ X \succ Y \lor Y \succ X \lor X = Y \]

We write $x \sim y$ when $x \succ y \land y \succ x$ holds.

Utility

Definition

A utility function corresponding to a preference preorder $\succeq S \times S$ is a function $u : S \rightarrow \mathbb{R}$ such that

\[ u(X) > u(Y) \iff X \succ Y \]

Remark

When the preferences are expressed over a set $S$ of investments that involve random events, then $S$ is a set of random variables.

The argument $X$ in a utility function $u(X)$ is usually a random variable.
Concave and convex functions

Definition
A function $f : V \rightarrow \mathbb{R}$ where $V$ is a vector space is
- convex if $f(aX + bY) \leq af(X) + bf(Y)$
- concave if $f(aX + bY) \geq af(X) + bf(Y)$
- linear if $f(aX + bY) = af(X) + bf(Y)$

Risk aversion formally

Definition
An investor whose preferences over a set of investments $S$ are expressed by a utility function $u : S \rightarrow \mathbb{R}$ is
- risk-seeking if $u$ is convex,
- risk-averse if $u$ is concave,
- risk-neutral if $u$ is linear.

Risk-seeking utility

- $W$ — wealth
- $E(W)$ — expected payoff: e.g., $\frac{1}{2} W_0 + \frac{1}{2} W_1$
- $RP$ — risk premium
- $CE$ — certainty equivalent: expected to be $E(W) - RP$

Risk-averse utility

- $W$ — wealth
- $E(W)$ — expected payoff
- $RP$ — risk premium
- $CE$ — certainty equivalent: expected to be $E(W) - RP$
Outline

Cost-Benefit Analysis for Security Investment

Security Risk Analysis

Level of Security Investment

Level of security investment

Question

How much should ToySec invest in security?

Model

Parameters

- $\ell = \text{loss}$: the value of the potential loss
- $t = \text{threat}$: probability of an attack
- $v = \text{vulnerability}$: probability that an attack will succeed, if it happens
  - $vt = \text{probability of a successful attack}$

Risk estimates

- $L = \ell \cdot t = \text{value under threat}$: fixed
- $v \cdot L = v \cdot \ell \cdot t = \text{expected loss with no security}$

Decreasing the vulnerability

- $x = \text{investment}$: the value of security investment
- $s(v, x) = \text{susceptibility}$: the vulnerability remaining from $v$ after the investment $x$

Benefit from investment in security

$$BIS(x) = (v - s(v, x))L$$
I-2. Security Investment
Dusko Pavlovic
Cost-Benefit
Security Risk
Investment

Net benefit from investment in security

\[ \text{NBIS}(x) = vL - s(v, x)L - x \]

Maximal net benefit

Idea

Since \( \text{NBIS}(x) = \text{BIS}(x) - x \), its maximum is reached at \( x^* \) such that

\[ \frac{d\text{NBIS}}{dx}(x^*) = 0 \iff \frac{d\text{BIS}}{dx}(x^*) = 1 \]

Maximal net benefit

The range of benefit

\[ \text{NBIS}(x^*) \geq 0 \land x^* \geq 0 \]
\[ \implies \text{BIS}(x^*) \geq x^* \geq 0 \]
\[ \implies (v - s(v, x^*))L \geq x^* \geq 0 \]
\[ \implies vL \geq x^* \geq 0 \]

Maximal net benefit

Assumptions about susceptibility

Question

Under which conditions is a maximal benefit achieved?

\[ s(0, x) = 0 \]
\[ s(v, 0) = v \]
\[ \frac{ds}{dx} < 0 \rightarrow s(v, x) \text{ decreases as } x \text{ increases} \]
\[ \frac{ds}{dx} > 0 \rightarrow \text{the rate of the decrease is decreasing} \]
Assumptions about susceptibility

- $s(0, x) = 0$
- $s(v, 0) = v$
- $\frac{\partial s}{\partial x} < 0$ — $s(v, x)$ decreases as $x$ increases
- $\frac{\partial^2 s}{\partial x^2} > 0$ — the rate of the decrease is decreasing
  - $s(v, x)$ is convex in $x$
  - there is $x^*$ such that $s(v, x^*) \leq s(v, x)$
  - there is $x^*$ such that $v - s(v, x^*) \geq v - s(v, x)$

Maximizing NBIS

\[ \frac{d\text{NBIS}}{dx}(x^*) = 0 \]
\[ \frac{\partial}{\partial x} (vL - s(v, x^*)L - x) = 0 \]

Optimal investment $x^*$ increases with $L$

(where $L = \ell$ is the value under threat)

\[ \frac{\partial s}{\partial x}(v, x^*) = \frac{1}{L} \]
\[ \frac{\partial^2 s}{\partial x^2}(v, x^*)dx = \frac{dL}{L^2} \]
\[ \frac{dx^*}{dL} = \frac{1}{L^2 \frac{\partial s}{\partial x}(v, x^*)} > 0 \]
Determining the optimal investment level

Decision procedure
1. estimate the parameters of your investment
   - loss ℓ
   - threat t
   - vulnerability v
2. pick a susceptibility function, such as:
   - \( s_I(v, x) = \frac{v}{(ax + 1)^b} \) for \( a > 0, b \geq 1 \)
   - \( s_{II}(v, x) = v^{ax} \) for \( a > 0 \)
3. tabulate BIS and NBIS for various \( x \)
4. try other choices of the parameters and the functions

Expected losses with susceptibility \( s_I \)

\[
\begin{array}{|c|c|c|c|c|}
\hline
x & s_I(v, x) & BIS(x) & NBIS(x) & \Delta BIS(x) \\
\hline
0 & .75 & 0 & 0 & - \\
65K & .5 & 250K & 195K & 55K \\
130K & .4 & 350K & 220K & 130K \\
195K & .33 & 420K & 250K & 70K \\
260K & .25 & 460K & 200K & 60K \\
\hline
\end{array}
\]

Rule of thumb

Proposition [Gordon-Loeb]

With the susceptibility functions from the classes \( s_I \) and \( s_{II} \), the optimal security investment \( x^* \) always satisfies

\[
x^* \leq \frac{\sqrt{L}}{a}
\]
Rule of thumb

Conclusion

The optimal security investment $x^*$ normally remains below 36% of the loss $v(t) = vL$ expected without any security investment.

Remark

This conclusion formally follows from the Proposition for all assets where the susceptibility functions $s'$ or $s''$ are applicable.

Similar conclusions follow from the extensions of the Proposition to other families of susceptibility functions.