Security & Economics — Part 2
Security Investment Analysis

Dusko Pavlovic

Spring 2014

Outline

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

Executive summary

Increase in cyber-threats keeps cost of breaches high

The vast majority of respondents had a security breach in the last year:

93%	of large organisations
76%	of small businesses

The main cause is an increase in the number of cyber-attacks, especially for large organisations:

54	is the median number of significant attacks by an unauthorised outsider on each large organisation in the last year (twice the level seen in 2010)
15%	of small businesses were hit by denial of service attacks in the last year
15%	of large organisations detected hackers had successfully penetrated their network in the last year

As a result, the cost to UK plc of security breaches remains high, while down somewhat on 2010 levels:

£15k - £30k	is the average cost of a small business's worst security breach of the year
£110k - £250k	is the average cost of a large organisation's worst security breach of the year
Billions	is the total cost to UK plc of security breaches in the last year

It's not just about technology – people are vital too

Most serious security breaches are due to multiple failings in people, processes and technology. Computer frauds, data losses and regulatory breaches (together with hacking attacks) were most likely to result in a very serious breach.

45%	of large organisations breached data protection laws in the last year (and this happened at least once a day at one in ten of them)
18%	of organisations affected by infringement of data protection laws had an effective contingency plan in place
20%	of small businesses lost confidential data (and 80% of these breaches were serious)
19%	of large organisations suffered from staff carrying out computer fraud

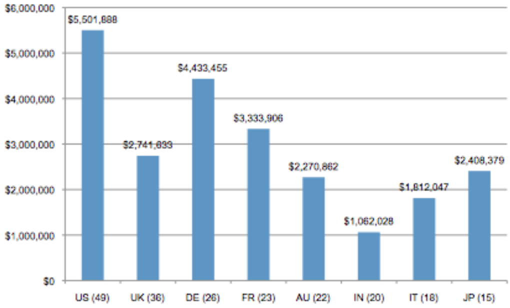
The root cause is often a failure to invest in educating staff about security risks, often only recognised after the event:

44%	of large organisations carried out additional staff training after their worst security breach of the year (and 38% changed their policies and procedures)
26%	of organisations with a security policy believe their staff have a very good understanding of it
75%	of organisations where the security policy was poorly understood had staff-related breaches
54%	of small businesses don't have any programme for educating their staff about security risks

Security has a major economic impact

Average organizational size of data breach. Figure 2 reveals the significant difference among countries in how much a data breach can cost an organization. From a high of $5.5 million in the US to a low of $1.1 in India, the costs are often dependent upon the type of data breach experienced by organizations and the country's regulatory landscape.

Figure 2. The average total organizational cost of data breach



Security has a major economic impact

eSecurityPlanet > Network Security > Security Breaches Cost $156.7 Billion Over Six Years

Security Breaches Cost $156.7 Billion Over Six Years

In 65 percent of cases, data disclosed included the data subject's name, address and social security number.

By **eSecurityPlanet Staff** | September 06, 2011

Share

A new study by the Digital Forensics Assocation has found that data breaches cost companies $156.7 billion over a six-year period.

"The study presents data breach information collected from 2005 through 2010, including the disclosure of more than 800 million records over that period," Infosecurity reports.

"In 65 percent of the data breach cases, the data disclosed included the subject's name, address, and social security number," the article states. "In contrast, only 15 percent of the incidents disclosed credit card numbers, and 16 percent disclosed medical information."

Go to "Data breaches cost organizations a staggering $156.7 billion over six years" to read the details.

For regular security news updates, follow eSecurityPlanet on Twitter: @eSecurityP.

White Papers | eBooks

2012 Bit9 Cyber Security Research Report

Anonymous hacktivists, cyber criminals and nation-states are viewed as the top three threats in 2012 in this Bit9 survey of more than 1,800 ...

Security has a major economic impact

Security is a business opportunity

Sex, Lies and Cyber-crime Surveys

Dinei Florêncio and Cormac Herley
Microsoft Research
One Microsoft Way
Redmond, WA, USA
{dinei,cormac}@microsoft.com

ABSTRACT

Much of the information we have on cyber-crime losses is derived from surveys. We examine some of the difficulties of forming an accurate estimate by survey. First, losses are extremely concentrated, so that representative sampling of the population does not give representative sampling of the losses. Second, losses are based on unverified self-reported numbers. Not only is it possible for a single outlier to distort the result, we find evidence that most surveys are dominated by a minority of responses in the upper tail (*i.e.*, a majority of the estimate is coming from as few as one or two responses). Finally, the fact that losses are confined to a small segment of the population magnifies the difficulties of refusal rate and small sample sizes. Far from being broadly-based estimates of losses across the population, the cyber-crime estimates that we have appear to be largely the answers of a handful of people extrapolated to the whole population. A single individual who claims \$50,000 losses, in an $N = 1000$ person survey, is all it takes to generate a \$10 billion loss over the population. One unverified claim of \$7,500 in phishing losses translates into \$1.5 billion.

1. INTRODUCTION

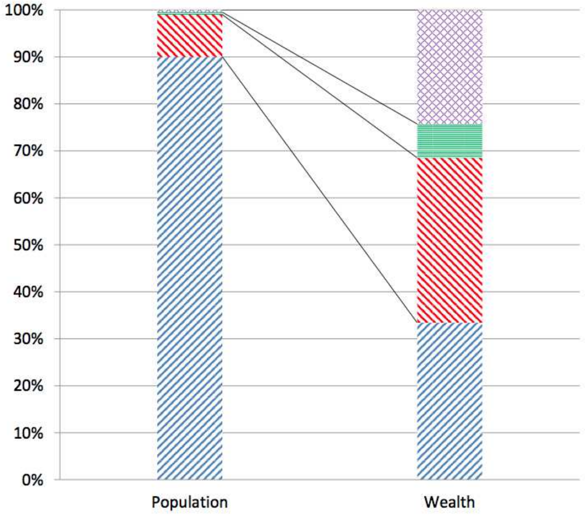
In the 1983 Federal Reserve Survey of Consumer Fi-

but eliminates the discrepancy.

How can this be? How can an estimate be so brittle that a single transcription error causes a \$1 trillion difference? How can two answers (in a survey of 5000) make a 3× difference in the final result? These cases have in common that the estimates are derived from surveys, that the underlying quantity (*i.e.*, wealth, ID theft losses, or number of sexual partners) is very unevenly distributed across the population, and that a small number of outliers enormously influenced the overall estimate. They also have in common that in each case, inclusion of the outliers, caused an enormous error to the upside, not the downside. It does not appear generally understood that the estimates we have of cyber-crime losses also have these ingredients of catastrophic error, and the measures to safeguard against such bias have been universally ignored.

The common way to estimate unknown quantities in a large population is by survey. For qualities which are evenly distributed throughout the population (such as voting rights) the main task is to achieve a representative sample. For example, if the achieved sample over- or under-represents any age, ethnic or other demographic group the result may not be representative of the population as whole. Political pollsters go to great lengths to achieve a representative sample of likely vot-
ers

Measurement influences the outcome



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

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
     - the *"due diligence" approach* does not suffice!

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

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

time	0	1	2	...
security benefit	B_0	B_1	B_2	...
security cost	C_0	C_1	C_2	...

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, 2013, ToySec buys a firewall for $200,000.
- During the year 2013, ToySec accumulates
  - firewall operating costs of $100,000, and
  - security benefits of $400,000

Basic accounting: Value

Net cash flow (NCF)

2013-01-01 - $200K

2014-01-01 $400K - $100K = $300K

Value (V) = total cash flow

2013-01-01 - $200K

2014-01-01 - $200K + $300K = $100K

Example 1'

- On January 1, *2014*, ToySec buys a firewall for $200,000.
- During the year *2014*, ToySec *is expected* to accumulate
  - firewall operating costs of $100,000, and
  - security benefits of $400,000

Basic accounting: *Future* Value

Net cash flow (NCF)

2014-01-01 - $200K

2015-01-01 $400K - $100K = $300K

Future value (FV) = total *expected* cash flow

2014-01-01 - $200K

2015-01-01 - $200K + $300K = $100K

Example 1 again

time	1-1-2013	1-1-2014
security benefit	0	$400,000
security cost	$200,000	$100,000

Example 1 again

time	1-1-2013	1-1-2014
security benefit	0	$400,000
security cost	$200,000	$100,000

$$\text{annual return on investment} = \frac{\text{investment profit}}{\text{investment cost}}$$

Example 1 again

time	1-1-2013	1-1-2014
security benefit	0	\$400,000
security cost	\$200,000	\$100,000

$$\text{annual return on investment} = \frac{\text{investment profit}}{\text{investment cost}} = \frac{\$(400,000 - 100,000)}{\$200,000} = 150\%$$

Concept 1: Annual return on investment (AROI)

Definition

Annual eturn 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

Concept 1: Annual return on investment (AROI)

Definition

Annual eturn 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

$$\text{AROI} = \frac{B_1 - C_1}{C_0}$$

Concept 1: Annual return on investment (AROI)

Decision rule

$\text{AROI} > 100\%$ — accept the investment

$\text{AROI} < 100\%$ — reject the investment

$\text{AROI} = 100\%$ — offers no grounds for a decision

Example 1 yet again

time	1-1-2013	1-1-2014
security benefit	0	\$400,000
security cost	\$200,000	\$100,000

$$\text{AROI} = \frac{(400,000 - 100,000)}{200,000} = 150\%$$

$\Longrightarrow$ invest!

Example 2

time	1-1-2013	1-1-2014
security benefit	0	$300,000
security cost	$250,000	$100,000

$$\text{AROI} = \frac{\$(300,000 - 100,000)}{\$250,000} = 80\%$$

$\Longrightarrow$ do not invest!

Example 3

time	1-1-2013	1-1-2014
security benefit	0	\$300,000
security cost	\$200,000	\$100,000

$$\text{AROI} = \frac{\$(300,000 - 100,000)}{\$200,000} = 100\%$$

$\Longrightarrow$ use a different accounting concept?

Accounting of security investments

Question

How do we calculate return on multi-period investments?

Example 4

- On January 1, 2014, ToySec buys an intrusion detection system for $200,000.
- During the year 2014 ToySec is expected to accumulate
  - firewall operating costs of $100,000, and
  - security benefits of $400,000

Example 4

- On January 1, 2014, ToySec buys an intrusion detection system for $200,000.
- During the year 2014 ToySec is expected to accumulate
  - firewall operating costs of $100,000, and
  - security benefits of $400,000
- During the year 2015 ToySec is expected to accumulate
  - firewall operating costs of $100,000, and
  - security benefits of $450,000

Example 4

time	1-1-2014	1-1-2015	1-1-2016
security benefit	0	$400,000	$450,000
security cost	$200,000	$100,000	$100,000

Example 4

time	1-1-2014	1-1-2015	1-1-2016
security benefit	0	\$400,000	\$450,000
security cost	\$200,000	\$100,000	\$100,000

$$\text{simple return on investment} = \frac{\text{total investment profit}}{\text{total investment cost}}$$

$$= \frac{(0 - 200) + (400 - 100) + (450 - 100)}{200 + 100 + 100}$$

$$= \frac{450}{400} = 112.5\%$$

Concept 1': Simple return on investment (SROI)

Definition

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

- total investment profit in a given period, obtained by subtracting
  - total costs $\sum_i C_i$ from
  - total benefits $\sum_i B_1$

  with
- total costs $\sum_i C_i$, needed to generate the profit

Concept 1': Simple return on investment (SROI)

Definition

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

- total investment profit in a given period, obtained by subtracting
  - total costs $\sum_i C_i$ from
  - total benefits $\sum_i B_1$

  with
- total costs $\sum_i C_i$, needed to generate the profit

$$\text{SROI} = \frac{\sum_i B_i - \sum_i C_i}{\sum_i C_i}$$

Concept 1': Simple return on investment (SROI)

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, 2014, ToySec buys an intrusion detection system for $200,000.
- During the year 2014 ToySec is expected to accumulate
  - firewall operating costs of $100,000, and
  - security benefits of $400,000

Example 4 again

- On January 1, 2014, ToySec buys an intrusion detection system for $200,000.
- During the year 2014 ToySec is expected to accumulate
  - firewall operating costs of $100,000, and
  - security benefits of $400,000
- During the year 2015 ToySec is expected to accumulate
  - firewall operating costs of $100,000, and
  - security benefits of $450,000

Example 4 again

- On January 1, 2014, ToySec buys an intrusion detection system for $200,000.
- During the year 2014 ToySec is expected to accumulate
  - firewall operating costs of $100,000, and
  - security benefits of $400,000
- During the year 2015 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.

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.

Concept 2: Net Present Value (NPV)

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

time	1-1-2014	1-1-2015	1-1-2016
security benefit	0	$400,000	$450,000
security cost	$200,000	$100,000	$100,000
cost of capital	15%		

Example 4

time	1-1-2014	1-1-2015	1-1-2016
security benefit	0	$400,000	$450,000
security cost	$200,000	$100,000	$100,000
cost of capital	15%		

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

$\Longrightarrow$ invest!

Example 5

time	1-1-2014	1-1-2015
security benefit	0	$400,000
security cost	$280,000	$100,000
cost of capital	15%	

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

$\Longrightarrow$ do not invest!

Example 6

time	1-1-2014	1-1-2015
security benefit	0	$400,000
security cost	$200,000	$100,000
cost of capital	50%	

$$\begin{aligned} \text{NPV} &= -200,000 + \frac{300,000}{1.5} \\ &= -200,000 + 200,000 \\ &= 0 \end{aligned}$$

$\Longrightarrow$ 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.

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.

$$0 = \sum_{t=0}^{n} \frac{B_t - C_t}{(1 + \mathrm{IRR})^t}$$

where usually $B_0 = 0$, except when there are instant benefits.

Concept 3: Internal rate of return (IRR)

Decision rule

Suppose that an investment *A* has a rate of return k_A.

$\text{IRR} > k_A$ — invest in security (not in *A*)

$\text{IRR} < k_A$ — do not invest in security (invest in *A*)

$\text{IRR} = k_A$ — consider other preferences

Example 7

- On January 1, 2014, ToySec buys an intrusion detection system for 280,000 .
- During the years 2015 and 2016 ToySec is expected to accumulate
  - firewall operating costs of $100,000 , and
  - security benefits of $400,000
- ToySec's cost of capital is 15%.

Example 7

time	1-1-2014	1-1-2015	1-1-2016
security benefit	0	\$400,000	\$400,000
security cost	\$280,000	\$100,000	\$100,000
rate of return of A	15%		

Example 7

time	1-1-2014	1-1-2015	1-1-2016
security benefit	0	\$400,000	\$400,000
security cost	\$280,000	\$100,000	\$100,000
rate of return of *A*	15%		

$$0 = -280,000 + \frac{300,000}{1+\mathrm{IRR}} + \frac{300,000}{(1+\mathrm{IRR})^2}$$

$$\Longrightarrow \quad \mathrm{IRR} = 70.12\% > 15\% = k_A$$

$\Longrightarrow$ invest in security!

Example 8

time	1-1-2014	1-1-2015
security benefit	0	\$400,000
security cost	\$280,000	\$100,000
cost of capital	15%	

$$0 = -280,000 + \frac{300,000}{1 + \text{IRR}}$$

$$\Longrightarrow \quad \text{IRR} = 7.14\% < 15\% = k_A$$

$$\Longrightarrow$$ invest in *A*!

Outline

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

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?

Example 1

Data

- You cannot tell whether an apple has a worm by looking at it.

Example 1

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.

Example 1

Solution: Probability

Denote the quality of the apple that you will pick by Q. Then

$$\begin{aligned}
\Pr(Q = \text{tasty}) &= \frac{18}{30} \\
\Pr(Q = \text{wormed}) &= \frac{8}{30} \\
\Pr(Q = \text{unripe}) &= \frac{4}{30}
\end{aligned}$$

Example 1

Formalization: Random variable

- The qualities of the available apples are viewed as a function $Q : \text{Apples} \to \text{Tastes}$

Example 1

Formalization: Random variable

- The qualities of the available apples are viewed as a function $Q : \text{Apples} \to \text{Tastes} = \{\text{unripe, tasty, wormed}\}$

Example 1

Formalization: Random variable

- The qualities of the available apples are viewed as a function Q : Apples $\to$ Tastes $=$ {unripe, tasty, wormed}
- Q induces a probability distribution $\Pr(Q=?)$: Tastes $\to [0,1]$ with the values

$$\Pr(Q = \text{tasty}) = \frac{\#\{a \in \text{Apples} \mid a \text{ tasty}\}}{\#\text{ Apples}} \approx \frac{18}{30}$$

$$\Pr(Q = \text{wormed}) = \frac{\#\{a \in \text{Apples} \mid a \text{ wormed}\}}{\#\text{Apples}} \approx \frac{8}{30}$$

$$\Pr(Q = \text{unripe}) = \frac{\#\{a \in \text{Apples} \mid a \text{ unripe}\}}{\#\text{Apples}} \approx \frac{4}{30}$$

Random variable

Definition

A random variable is a function

$$X \quad : \quad A \to V$$

which induces a probability distribution $\Pr(X =?) : V \to [0, 1]$ where

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

Random variable

Explanation

- Algebraic variable x in $x^2 - 1 \in \mathbb{Z}[x]$ denotes an *indeterminate* value $a \in \mathbb{R}$
  - later determined by assignment $x = a$
- Random variable X in $X^2 + 3X + 1 \in \mathbb{Z}[X]$ denotes an *indeterminate* value $a \in \mathbb{R}$
  - later determined by sampling $X = a$
  - according to the probability distribution on $\mathbb{Z}$ induced by X.

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

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 would you pay for insurance?

Example 2

Data

apple quality	tasty	wormed	unripe
loss	0 ¢	100 ¢	50 ¢
probability	$\frac{18}{30}$	$\frac{8}{30}$	$\frac{4}{30}$

Example 2

Data

apple quality	tasty	wormed	unripe
loss	0 ¢	100 ¢	50 ¢
probability	$\frac{18}{30}$	$\frac{8}{30}$	$\frac{4}{30}$

Solution: Expected value of the loss

$$\begin{aligned}\text{expected loss per apple} &= \frac{18}{30}\cdot 0 + \frac{8}{30}\cdot 100 + \frac{4}{30}\cdot 50 \\ &= 33.3\end{aligned}$$

Example 2

Formalization: Expected value

- The random variable $L : \text{Apples} \to \mathbb{R}$ is distributed as follows

$$
\begin{aligned}
\Pr(L = 0) &= \frac{18}{30} \\
\Pr(L = 100) &= \frac{8}{30} \\
\Pr(L = 50) &= \frac{4}{30} \\
\Pr(L = \text{other}) &= 0
\end{aligned}
$$

- The expected value of the random variable L is

$$
\begin{aligned}
\int_{Apples} L &= \sum_{r \in \mathbb{R}} r \cdot \Pr(L = r) \\
&= 100 \cdot \frac{8}{30} + 50 \cdot \frac{4}{30} = 33.3
\end{aligned}
$$

Expected value

Definition

The expected value of a random variable $X : A \to \mathbb{R}$

$$\int_A X \quad = \quad \sum_{x \in A} X(x) \cdot \Pr(x)$$

Expected value

Proposition

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

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

What is risk?

Definition

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

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)

Example 3

Problem: Quantifying the IT risk

Type of incident:	Losses:
denial of service (DoS)	\$1M
loss of data (LD)	\$2M
loss of IP (LIP)	\$3M

Example 3

Data: ToySec Admin. Dept. A

incident	DoS	LD	LIP
cost	1M	2M	3M
probability	0	.06	0

Example 3

Data: ToySec Admin. Dept. A

incident	DoS	LD	LIP
cost	1M	2M	3M
probability	0	.06	0

Risk: Expected loss

$$\begin{aligned} \int \text{loss}_A &= .06 \cdot 2,000,000 \\ &= 120,000 \end{aligned}$$

Example 4

Data: ToySec Design Dept. D

incident	DoS	LD	LIP
cost	1M	2M	3M
probability	0	0	.04

Risk: Expected loss

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

Example 4

Data: ToySec Sales Dept. S

incident	DoS	LD	LIP
cost	1M	2M	3M
probability	.06	.015	.01

Risk: Expected loss

$$
\begin{aligned}
\int \text{loss}_S &= .06 \cdot 1,000,000 \\
&\quad +.015 \cdot 2,000,000 \\
&\quad +.01 \cdot 3,000,000 \\
&= 120,000
\end{aligned}
$$

Comparison

Question

- Are all three departments at the same risk?

Comparison

Overview

incident	DoS	LD	LIP
cost	1M	2M	3M
probability for ToySec A	0	.06	0
probability for ToySec D	0	0	.04
probability for ToySec S	.06	.015	.01

Comparison

Overview

incident	DoS	LD	LIP
cost	1M	2M	3M
probability for ToySec A	0	.06	0
probability for ToySec D	0	0	.04
probability for ToySec S	.06	.015	.01

Observations

- *D* and *S* may lose 3M
- *S*'s total loss probability is .085
- ...

Comparison

Question

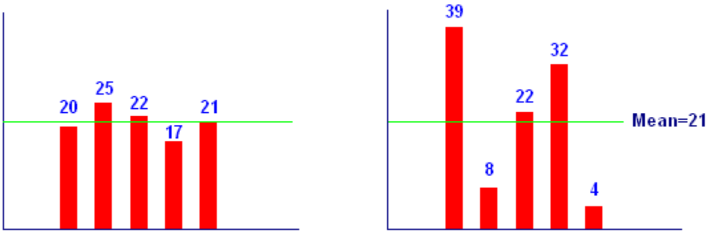
- Is the average (expected value of) loss a good measure of risk?

Comparison

Question

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

Deviation



Absolute deviation

Definition

The *absolute deviation* of a random variable $X : A \to \mathbb{R}$ is

$$\alpha(X) \quad = \quad \int_{x \in A} \left| X - \int_{x \in A} X \right|$$

Absolute deviation

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 $X : A \to \mathbb{R}$ is

$$\sigma(X) = \sqrt{\int_{x \in A} \left(X - \int_{x \in A} X \right)^2}$$

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

Variance

Definition

The *variance* of a random variable $X : A \to \mathbb{R}$ is the square of its standard deviation:

$$\mathrm{Var}(X) \quad = \quad \int_{x \in A} \left(X - \int_{x \in A} X \right)^2$$

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

α, σ and Var induce the same order on random variables:

$$
\begin{array}{rcl}
\alpha(X) & \leq & \alpha(Y) \\
& \Updownarrow & \\
\sigma(X) & \leq & \sigma(Y) \\
& \Updownarrow & \\
\mathrm{Var}(X) & \leq & \mathrm{Var}(Y)
\end{array}
$$

Conclusion

Absolute deviation, standard deviation and variance

- measure how well a random variable fits its expected value
- σ and Var are correspond to normally distributed (Gaussian) deviations and have a simpler statistic than α
- $\sigma(X)$ and $\alpha(X)$ are the same units as X, whereas $\mathrm{Var}(X)$ 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 $A \succ B \succ C$

risk-averse if your preference order is $C \succ B \succ A$

risk-neutral if you are indifferent between the three gambles, i.e. $A \sim B \sim C$

Risk aversion informally

Question

Is there any situation in which your preference order could be

- $B \succ C \succ A$
- $B \succ A \succ C$
- $A \succ C \succ B$
- $C \succ A \succ B$

?

Risk aversion

Similar example?

You are given 3 choices:

- A: a lottery where you have a 1 in 1,000,000 chance to win $ 1,000,000
- B: a 1 in 100 chance to win $ 100 shoes
- C: you get $ 1 for sure

What would you choose?

Problems of security managers

Security decisions require rational decisions

- evaluating risk

Problems of security managers

Security decisions require rational decisions

- evaluating risk

  $\Uparrow$

- determining your risk position

Problems of security managers

Security decisions require rational decisions

- evaluating risk

  $\Uparrow$

- determining your risk position

  $\Uparrow$

- specifying your preferences and utility

Problems of security managers

Security decisions require rational decisions

- evaluating risk

  $\Uparrow$

- determining your risk position

  $\Uparrow$

- specifying your preferences and utility

It gets harder and harder.

Problems of security managers

Security decisions require rational decisions

- evaluating risk

  $\Uparrow$
- determining your risk position

  $\Uparrow$
- specifying your preferences and utility

It gets harder and harder. Need math!

Preference

Definition

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

$$X \succ Y \ \wedge \ Y \succ Z \implies X \succ Z$$
$$X \succ Y \ \vee Y \succ X \ \vee X = Y$$

Preference

Definition

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

$$X \succ Y \ \wedge \ Y \succ Z \implies X \succ Z$$
$$X \succ Y \ \vee Y \succ X \ \vee X = Y$$

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

Utility

Definition

A *utility function* corresponding to a preference preorder $\succ \subseteq \mathcal{S} \times \mathcal{S}$ is a function $u : \mathcal{S} \to \mathbb{R}$ such that

$$u(X) > u(Y) \iff X \succ Y$$

Utility

Remark

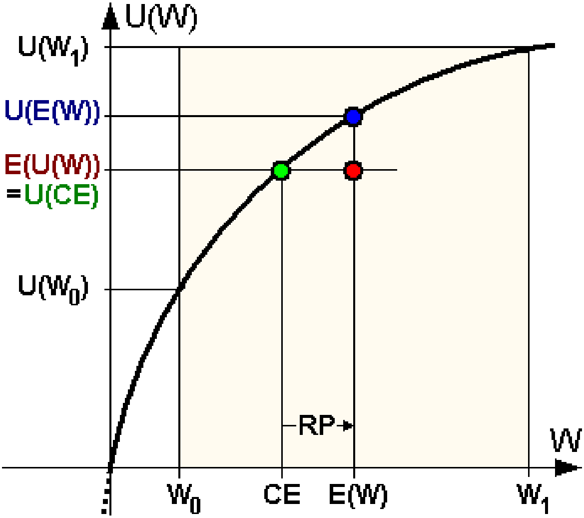
When the preferences are expressed over a set $\mathcal{S}$ of investments that involve random events, then $\mathcal{S}$ is a set of random variables.

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

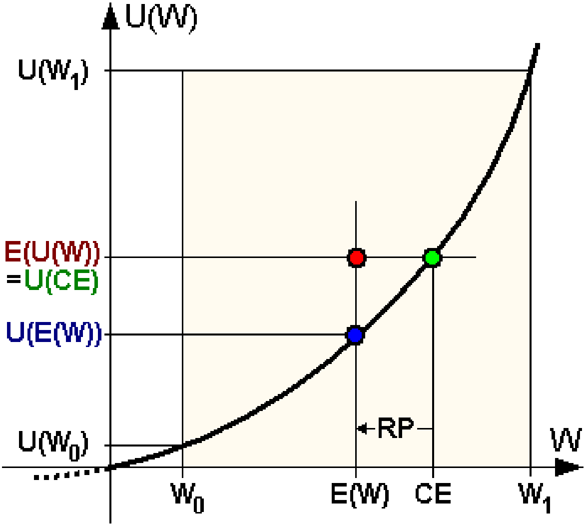
Risk aversion formally

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

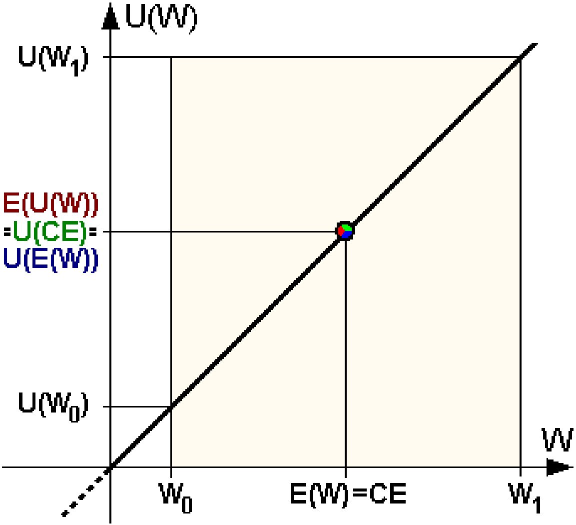
Risk-averse utility



Risk-seeking utility



Risk-neutral utility



Concave and convex functions

Definition

A function $f : \mathcal{V} \to \mathbb{R}$ where $\mathcal{V}$ 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 $\mathcal{S}$ are expressed by a utility function $u : \mathcal{S} \to \mathbb{R}$ is

risk-seeking if u is convex,

risk-averse if u is concave,

risk-neutral if u is linear.

Outline

Level of security investment

Question

How much should ToySec invest in security?

Model

Parameters

- ℓ = **loss:** the value of the potential loss
- t = **threat:** probability of an attack
- v = **vulnerability:** probability that an attack will succeed, if it happens
  - vt = probability of a successful attack

Model

Parameters

- ℓ = **loss:** the value of the potential loss
- t = **threat:** probability of an attack
- v = **vulnerability:** probability that an attack will succeed, if it happens
  - vt = probability of a successful attack

Risk estimates

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

Decreasing the vulnerability

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

Benefit from investment in security

$$\mathrm{EBIS}(x) \quad = \quad \big(v - s(v,x)\big)L$$

Net benefit from investment in security

$$\text{NBIS}(x) \quad = \quad vL - s(v,x)L - x$$

Maximal net benefit

Idea

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

$$\frac{d\text{NBIS}}{dx}(x^*) = 0 \iff \frac{d\text{EBIS}}{dx}(x^*) = 1$$

Maximal net benefit

The range of benefit

$$\mathrm{NBIS}(x^*) \geq 0 \ \wedge \ x^* \geq 0$$

$$\Updownarrow$$

$$\mathrm{EBIS}(x^*) \geq x^* \geq 0$$

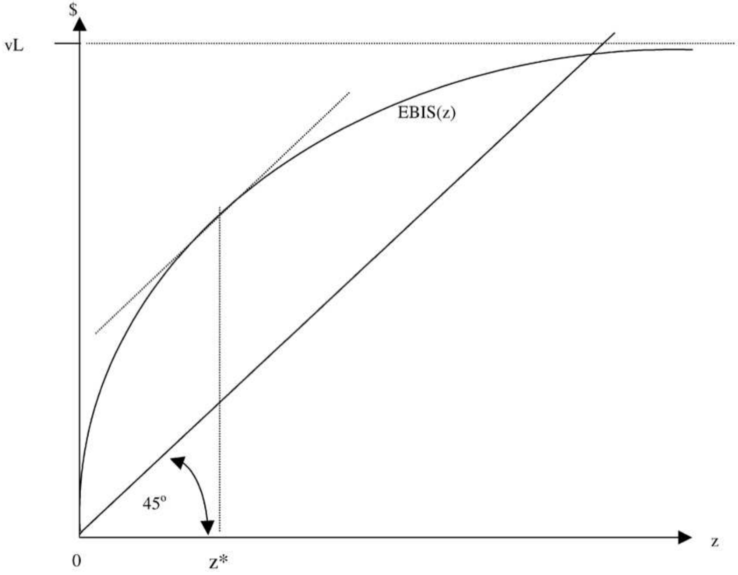
$$\Updownarrow$$

$$\big(v - s(v, x^*)\big)L \geq x^* \geq 0$$

$$\Uparrow$$

$$vL \geq x^* \geq 0$$

Maximal net benefit



Maximal net benefit

Question

Under which conditions is a maximal benefit achieved?

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

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

$$\frac{d\mathrm{NBIS}}{dx}(x^*) \quad = \quad 0$$

Maximizing NBIS

$$\frac{d\text{NBIS}}{dx}(x^*) = 0$$

$$\Updownarrow$$

$$\frac{\partial}{\partial x}\left(vL - s(v, x^*)L - x\right) = 0$$

Maximizing NBIS

$$
\begin{aligned}
\frac{d\text{NBIS}}{dx}(x^*) &= 0 \\
&\Updownarrow \\
\frac{\partial}{\partial x}\left(vL - s(v, x^*)L - x\right) &= 0 \\
&\Updownarrow \\
-L\frac{\partial s}{\partial x}(v, x^*) &= 1
\end{aligned}
$$

Maximizing NBIS

$$
\begin{array}{rcl}
\frac{d\text{NBIS}}{dx}(x^*) & = & 0 \\
& \Updownarrow & \\
\frac{\partial}{\partial x}\left(vL - s(v, x^*)L - x\right) & = & 0 \\
& \Updownarrow & \\
-L\frac{\partial s}{\partial x}(v, x^*) & = & 1 \\
\uparrow & & \uparrow
\end{array}
$$

marginal benefit of x marginal cost of x

Optimal investment x^* increases with L

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

$$\frac{\partial s}{\partial x}(v, x^*) = -\frac{1}{L}$$

$$\Downarrow$$

$$\frac{\partial^2 s}{\partial x^2}(v, x^*)dx^* = \frac{dL}{L^2}$$

$$\Downarrow$$

$$\frac{dx^*}{dL} = \frac{1}{L^2 \frac{\partial^2 s}{\partial x^2}(v, x^*)} > 0$$

Determining the optimal investment level

Decision procedure

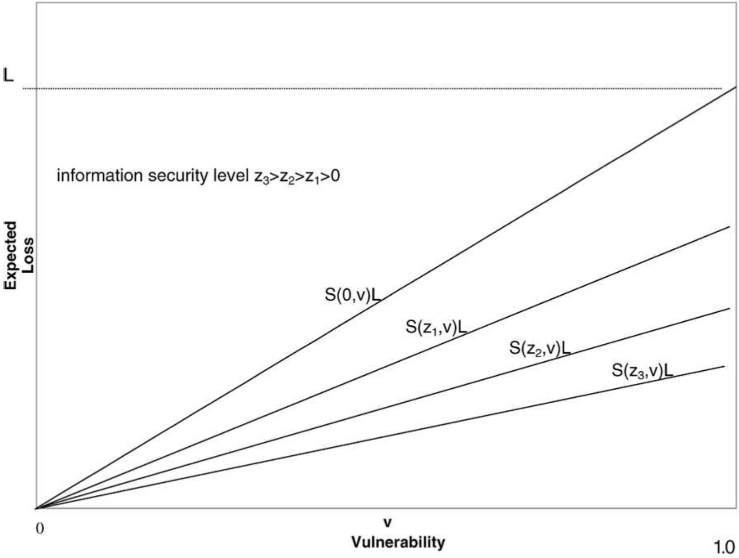
1. estimate the parameters of your investment
   - loss ℓ
   - threat t
   - vulnerability v

2. pick a susceptibility function, such as:
   - $s^I(v,x) = \frac{v}{(ax+1)^b}$ for $a > 0$, $b \geq 1$
   - $s^{II}(v,x) = v^{1-ax}$ for $a > 0$

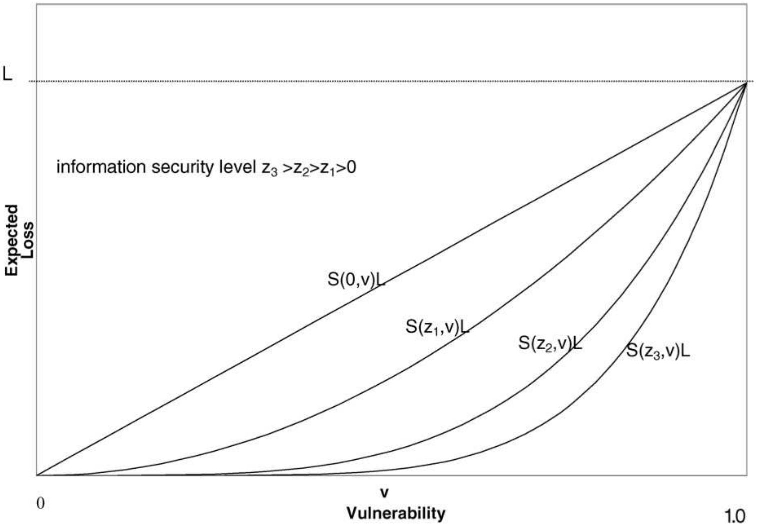
3. tabulate EBIS and NBIS for various x

4. try other choices of the parameters and the functions

Expected losses with susceptibility s^l



Expected losses with susceptibility s^{II}



Susceptibility classes

Remark

- The family s^{I} suffices for most assets
  - the security expense grows linearly with v
- The family s^{II} is suitable for highly sensitive assets
  - the security expense grows exponentially with v

Tabulating EBIS and NBIS

For $\ell = 1000K$ and $v = .75$

x	s(v,x)	EBIS(x)	NBIS(x)	ΔEBIS(x)	ΔNBIS(x)
0	.75	0	0	–	–
65K	.5	250K	195K	250K	195K
130K	.4	350K	220K	100K	35K
195K	.33	420K	225K	70K	5K
260K	.29	460K	200K	40K	-25K

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

$$x^* \leq \frac{vL}{e}$$

Rule of thumb

Conclusion

The optimal security investment x^* normally remains below 36% of the loss $vt\ell = vL$ expected without any security investment.

Rule of thumb

Conclusion

The optimal security investment x^* normally remains below 36% of the loss $vt\ell = vL$ expected without any security investment.

Remark

This conclusion formally follows from the Proposition for all assets where the susceptibility functions s^I or s^{II} are applicable.

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