Cost Benefit Analysis

Cost-benefit framework

- CBA
  - widely accepted economic principle for managing organizational resources
  - Requires cost of activity compared with the benefit
    - Cost > Benefit?
    - Cost < Benefit?
    - Cost = Benefit?

Cyber security Cost

- Operating Cost
  - Expenditure that will benefit a single period's operations (one fiscal year)
    - E.g., cost of patching software to correct breaches in the fiscal year

- Capital Investment
  - Expenditure that will benefit for several periods (Appears in balance sheet)
  - E.g., purchase of an IDS system (+ personnel cost)
    - Expect to work at least next few years

Cyber security Cost

- Capital investments lose their economic values
  - Portion of the investment that has been lost during a particular period is charged to that period

- In practice,
  - the distinction is not straightforward
  - Some argue
    - Most Cyber security expenditure are operating costs
    - However, they have spill over effect – hence could be treated as capital investment

Middle ground!!

Cyber security Cost : In practice

- Most org. treat cyber security expenditure as Operating costs
  - Accounting and tax rules allow/motivate
    - By expensing these costs in the year of expenditure, tax savings are realized immediately

- Distinction is good (recommended)
  - From planning perspective

- A good approach
  - View all as capital investments with varying time horizons
  - OC becomes a special case of CI

Cost (C) vs. Benefit (B)

- Assume
  - B and C can be assessed for different level of cyber security activities
- Organization's goals should be
  - Implement security procedures up to the point where (B-C) is maximum
  - Implementing beyond that point means
    - The incremental costs > the incremental benefits
      - Net benefit beyond that maximum point is negative

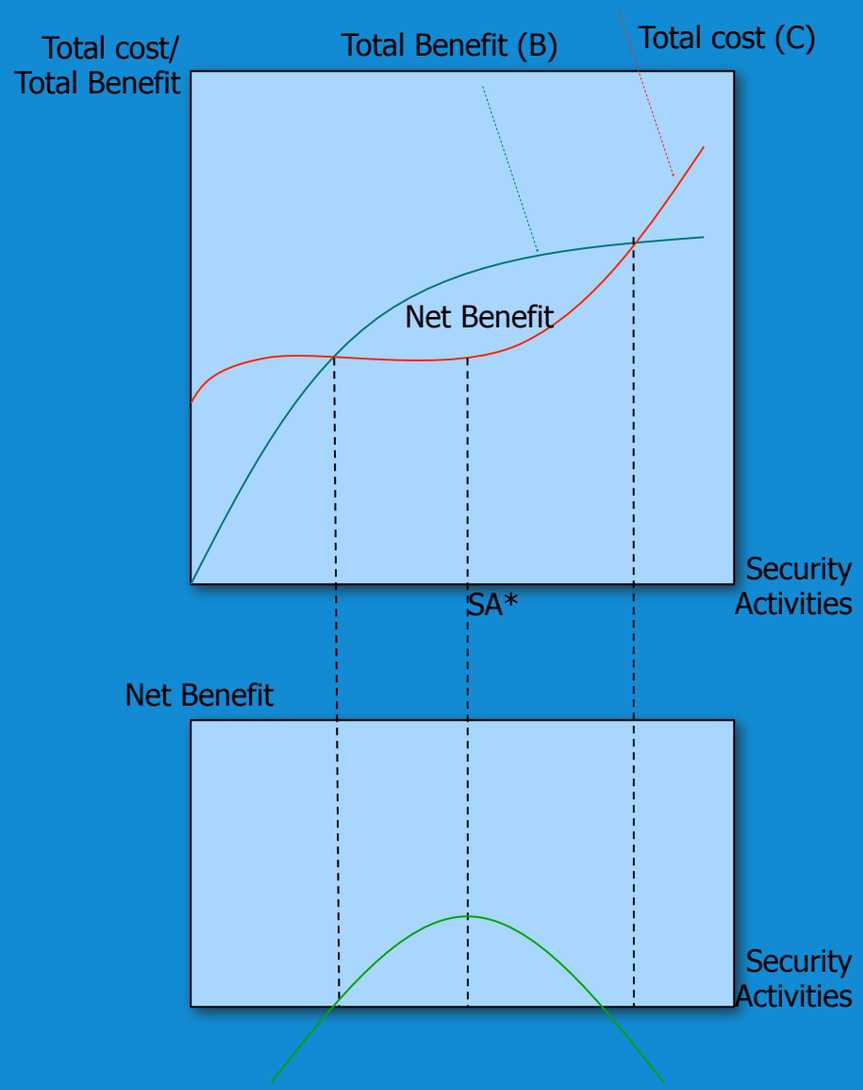
Cost (C) vs. Benefit (B)

- Cost-Benefit principle
  - Keep increasing security activities as long as the incremental benefits exceed their incremental costs

- If security activities can be increased in small amounts
  - Such activities should be set at the point where the incremental (cost = benefit)

Cost vs Benefit

- Security activities are increasing at decreasing rate
  - There are diminishing associated marginal benefits
- Can assume that C has
  - Fixed portion (irrespective of levels of activities)
  - Variable portion (varies with the level of activities)
    - Assume to initially increase at decreasing rate and then increase at increasing rate



Net Present Value Model

- C and B can be quantified in terms of Net Present Value (NPV)

- NPV
  - Financial tool for comparting anticipated benefits and costs voer different time periods
  - Good way to put CBA into practice

Net Present Value Model

- To compute NPV,
  - First discount all anticipated benefits and costs to today's value or present value (PV)
  - NPV = PV – Initial cost of the project

- Key aspect of NPV model
  - Compare the discounted cash flows associated with the future benefits and costs to the initial cost of an investment
    - All costs are in monetary unit

Net Present Value Model

$$NPV = -C_o + \sum_{t=1}^{n} (B_t - C_t)/(1+k)^t$$

Net Present Value Model

- C_o:
  - Cost of initial investment
- B_t and C_t:
  - anticipated benefits and costs, resp., in time period t from the additional security activities
- k:
  - Discount rate, which is usually considered an organization's cost of capital
  - It indicates the minimum rate a project needs to earn in order that the organization's value will not be reduced

- NPV model is most easily considered in terms of incremental investments

- Realistic situation is
  - Some level of security is already in place (e.g., basic firewalls, access controls)
  - It can be used to compare the incremental costs with incremental benefits associated with increases in SA

Net Present Value Model

- NPV greater than zero
  - Accept the incremental security activities
- NPV less than zero
  - Accept the incremental security activities
- NPV = zero
  - Indifference
- k can be used to model risk

Internal Rate of Return (IRR) Model

$$C_o = \sum_{t=1}^{n} (B_t - C_t)/(1 + IRR)^t$$

- Also known as economic rate of return
- *IRR:* Is the discount rate that makes the NVP = zero, thus:
- Decision
  - $IRR > k$, accept the SA
  - $IRR < k$, reject
  - $IRR = k$, indifference
- To select security investments
  - NVP ranking is preffered than IRR ranking

Must-do Projects

- Some SA are required by law and hence must be done
  - Irrespective of IRR/NVP

- Example
  - HIPAA compliance requirements
    - Safeguards must be in place to provide authorized access to patient information
    - Many outsource SA

Example 1

- Organization wants a new IDS
  - Initial investment is $200,000
    - Beginning of the first period
  - Expected to have a two-year useful life
  - Annual increment benefits generated from the investment is estimated = $400,000
  - Annual incremental operating cost for the system is estimated to be $100,000.
  - Discount rate: 15%

A.

Net Present Value (discount rate = 15%)

	C_0	t_1	t_2
Initial investment	–$200,000		
Annual benefits (i.e., cost savings)		$400,000	$400,000
Annual operating costs	_____	–$100,000	–$100,000
Net cash flow	–$200,000	$300,000	$300,000

$$\text{NPV} = -\$200{,}000 + \frac{\$300{,}000}{(1.15)^1} \quad \frac{\$300{,}000}{(1.15)^2}$$

$$\text{NPV} = -\$200{,}000 + \$260{,}870 + \$226{,}843$$

NPV = $287,713

B.

Internal Rate of Return

	C_0	t_1	t_2
$0 = -\$200{,}000 + \frac{\$300{,}000}{1 + \text{IRR}} + \frac{\$300{,}000}{(1 + \text{IRR})^2}$			

$$\$200{,}000 = \frac{\$300{,}000}{1 + \text{IRR}} + \frac{\$300{,}000}{(1 + \text{IRR})^2}$$

IRR = 118.61%

A.

Net Present Value (discount rate = 15%)

	C_0	t_1
Initial investment	–$200,000	
Annual benefits (i.e., cost savings)		$400,000
Annual operating costs		–$100,000
Net cash flow	–$200,000	$300,000

$$\text{NPV} = -\$200{,}000 + \frac{\$300{,}000}{(1.15)^1}$$

$$\text{NPV} = -\$200{,}000 + \$260{,}870$$

NPV = $60,870

B.

Internal Rate of Return

	C_0	t_1
	$0 = -\$200{,}000 + \frac{\$300{,}000}{1 + \text{IRR}}$	

$$\$200{,}000 = \frac{\$300{,}000}{1 + \text{IRR}}$$

IRR = 50.00%

Example 2

- Initial investment is $280,000
  - Beginning of the first period
- Expected to have a two-year useful life
- Annual increment benefits generated from the investment is estimated = $400,000
- Annual incremental operating cost for the system is estimated to be $100,000.
- Discount rate: 15%

A.

Net Present Value (discount rate = 15%)

	C_0	t_1	t_2
Initial investment	–$280,000		
Annual benefits (i.e., cost savings)		$400,000	$400,000
Annual operating costs	_____	–$100,000	–$100,000
Net cash flow	–$280,000	$300,000	$300,000

$$NPV = -\$280{,}000 + \frac{\$300{,}000}{(1.15)^1} + \frac{\$300{,}000}{(1.15)^2}$$

$$NPV = -\$280{,}000 + \$260{,}870 + \$226{,}843$$

NPV = $207,713

B.

Internal Rate of Return

	C_0	t_1	t_2
0 =	–$280,000 +	$\frac{\$300{,}000}{1 + IRR}$ +	$\frac{\$300{,}000}{(1 + IRR)^2}$

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

IRR = 70.12%

A.

Net Present Value (discount rate = 15%)

	C_0	t_1
Initial investment	–$280,000	
Annual benefits (i.e., cost savings)		$400,000
Annual operating costs		–$100,000
Net cash flow	–$280,000	$300,000

$$\text{NPV} = -\$280{,}000 + \frac{\$300{,}000}{(1.15)^1}$$

$$\text{NPV} = -\$280{,}000 + \$260{,}870$$

NPV = –$19,130

B.

Internal Rate of Return

	C_0	t_1
	$0 = -\$280{,}000 + \frac{\$300{,}000}{1 + \text{IRR}}$	

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

IRR = 7.14%

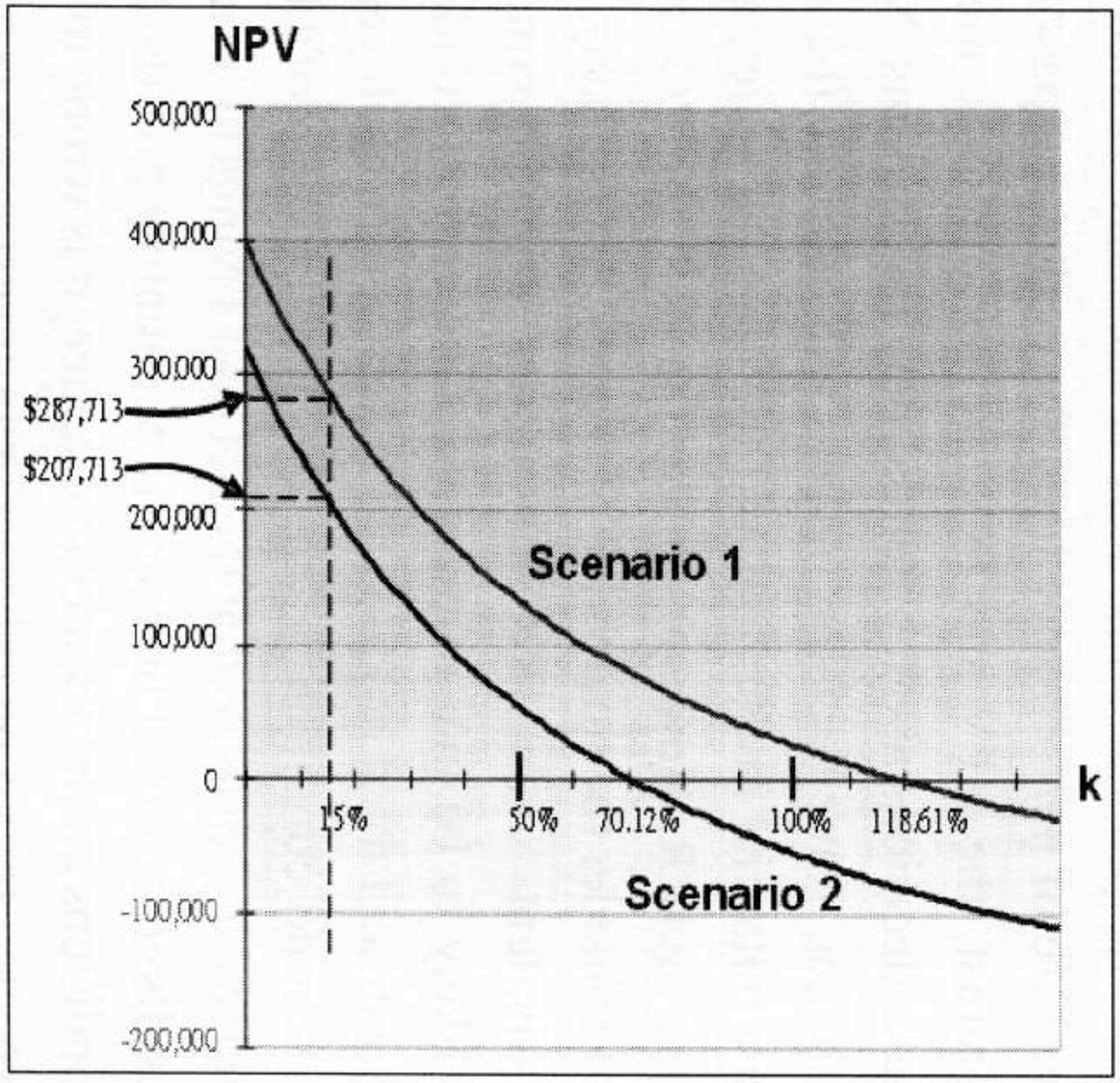
More on k

- Higher k means lower NVP
  - Attractiveness of SA will be related to k

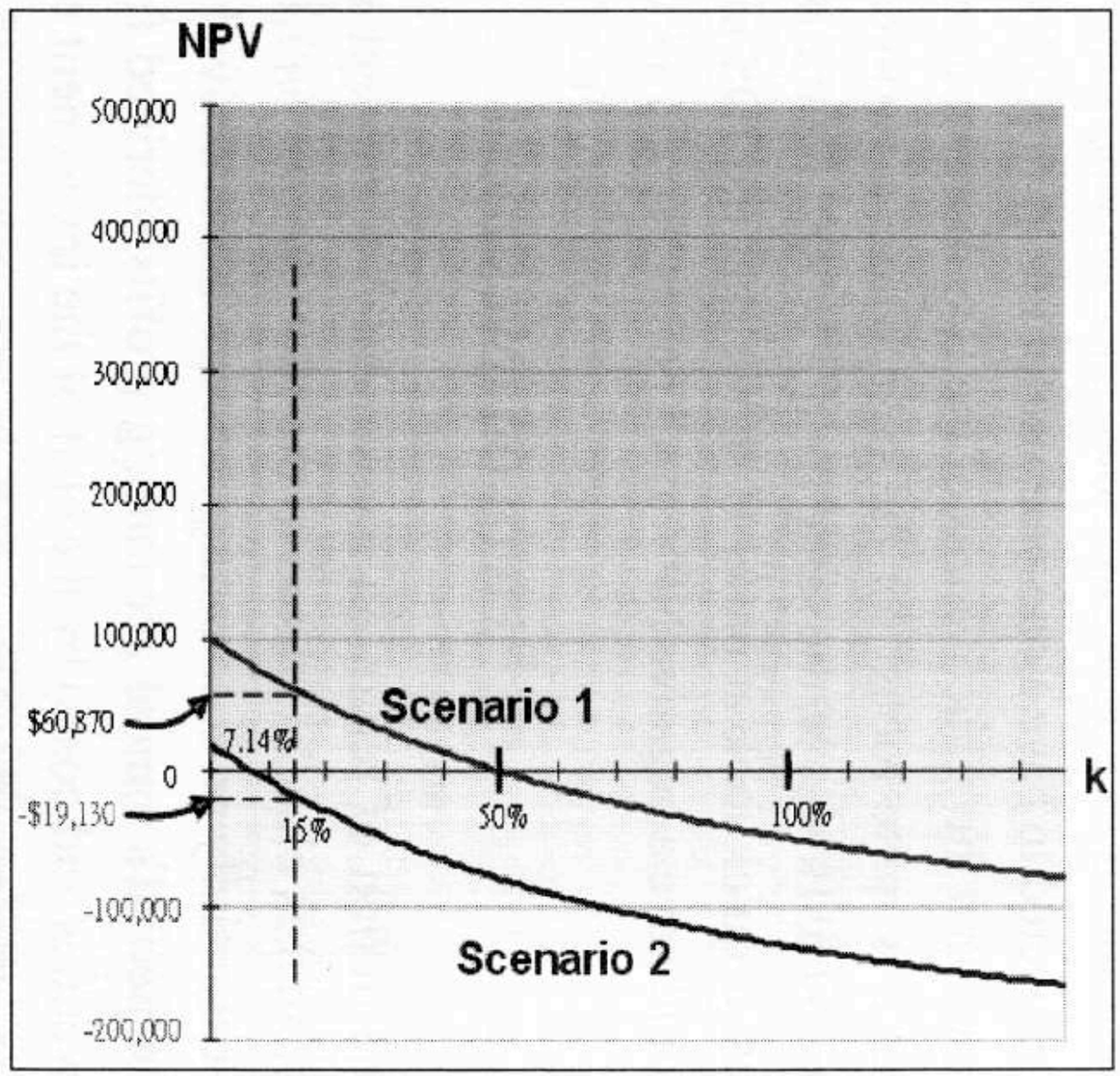
- Most corporations use
  - weighted-average cost of capital (WC) in discounting future cash flows
  - For risky projects, some premiums may be added
  - E.g., WC = 15 and k = 20

NPV Comparative Charts

A. Two-year Useful Life



B. One-year Useful Life



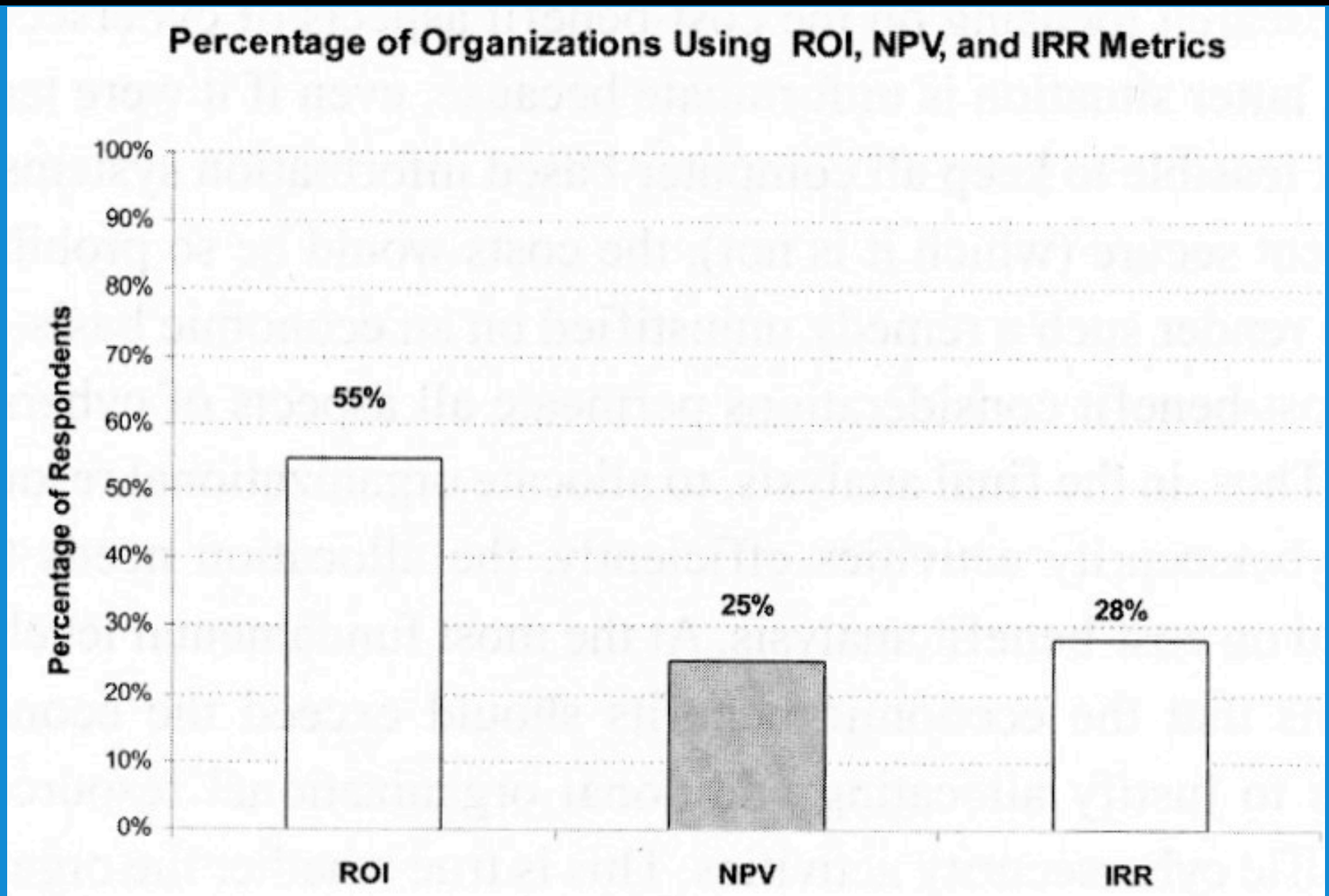
Return on Investment

- ROI is essentially
  - Last period's annual profits
  - divided by
  - cost of the investment required to generate the profit
- ROI viewed as
  - Historical measure of performance used for evaluating past investments
- NPV & IRR
  - Performance measures used to make decisions about potential new investments
  - Unlike IRR, ROI technically does not consider time value of money

Return on Investment

- ROIs for the two examples
  - Example 1: 300K/200K * 100% = 150%
  - Example 2: 300K/280K * 100% = 107%
- ROI assumes that
  - The investment will continue to produce returns of $300 for year 2, 3, 4 & beyond
  - Dramatically overstates the economic rate of return.
  - The more that the returns persist, the better the ROI is an approximation of the IRR
    - If 300K net benefit could go on forever, the ROI = IRR
- Survey shows,
  - Many managers are using ROI acronyms to represent IRR

Introduction



ROI = return on investment

NPV = net present value

IRR = internal rate of return