

# *“Advantages in defining and adopting a security policy”*

*Information & Network Security Workshop - Bologna, 1<sup>st</sup> July 2003*



**Speaker: Angelo Perniola - Infosec Project Manager**  
**perniola@infosec.it**

# Agenda

- WHAT** information as an asset, security issues (CIA), security policies
- WHY** investment not cost, ROSI, value of trust
- HOW** effective policies & examples

# Information assets

**“Information today lie at the core of business ....”**

**... ever bought an IDC report ?**

✓ What's the hardest task managers face everyday ?

**“Decision Making”**

✓ What's the most powerful help managers can get in DM ?

**“The right information (at the right time)”**

✓ Information need to be “collected” first but then “protected”

# Security Issues

## Goal:

Preservation of **C.I.A.** ...



... but **Confidentiality, Integrity, Availability**

## Implications of lack of security related to information:

1. **Business:** loss of money (loss of transaction capability, patents, share value, reputation, relationships with partners, ...);
2. **Legal:** Compliance with legislation (privacy, customer data, ...), Respecting contract agreements (SLA, ...), Intellectual property issues;
3. **Intangibles:** how do we measure the cost of trust (internal and external) ? And the cost of privacy?

...

- n **Loss of competitive advantage** (business, research, education, ...)

# Security Policy

## Definition

A **document** that outlines specific requirements that must be met in order to protect information assets.

**CONFIDENTIALITY**



Who can access information

**INTEGRITY**



How/when information can be altered

**AVAILABILITY**



How/when information can be accessed

## Why we need a security policy

It defines what is "**secure**" for a system/set of systems → It is the foundation of information security.

... What about the business ?

# Advantages of security policies

## The right balance:

- For security people: security is a “**necessity**” no matter what !!!
- For business people: security is a “**cost**” and nothing else !!!
- As usual, the truth lies in between:

“**set of operational business processes** (just like sales, customer service, logistics, ...)”

## Where is the value:

- 1) ROSI
- 2) Trust

# Advantages of security policies [cont.]

## ROSI (Return On Security Investment):

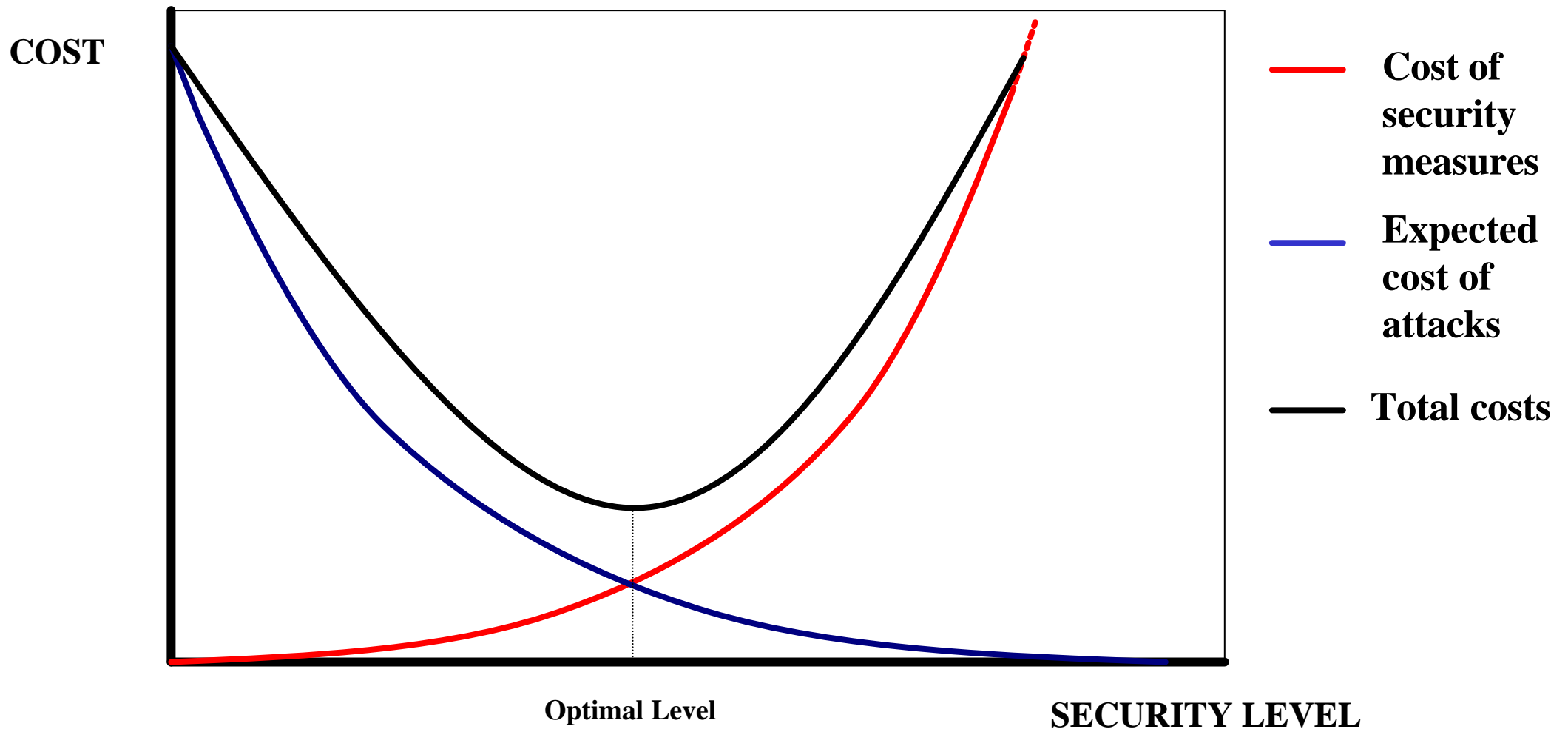
- Still a smoky point
- Involves a lot of intangibles
- $ROSI = \frac{\text{Change in Revenue} + \text{Cost Savings}}{\text{Investment}}$

It requires a large "case history" (see auto insurances for theft)

## Trust:

- Globalization (information flows, no boundaries, ...)
- Slow economic times (invest where you trust)
- Partnerships (choose appropriate partners)
- e-insurance (like Lloyd's 300 yrs. ago, lower premiums)

# Security Cost Function



Source: *A Structured Approach to Computer Security*, T. Olovsson, 1992.

*Advantages in defining and adopting a security policy - Page 8*

© 2003 Infosec srl – All rights reserved. No copies allowed without permission.

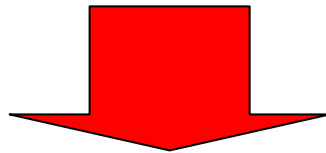
# Costs quantification

## How do we measure costs of security measures ?

- Know what to protect
- Know how to protect it (not only technology !!!)

## How do we measure costs of eventual attacks

- Know how likely threats are
- Know how valuable assets are



**Set the goal !!!**

**(... and it's not - only - a technical issue)**

# Costs quantification [cont.]

## Some key tradeoffs in determining our security goals

- Services offered vs. Security provided
- Ease of use vs. Security
- Access control vs. Accountability
- Cost of security vs. Risk of loss

## Problems: hidden costs

- Inefficiencies
- Excessive protections
- Loss of opportunities
- ... the best result is when nothing happens

# Investments

Investments are there ...

Security Technology Used (% of respondents)	1999	2001	2003
	Firewall	91%	95%
Intrusion Detection Systems	42%	61%	73%
Antivirus	98%	98%	99%
Encrypted Login	46%	53%	58%

... but they are not very effective

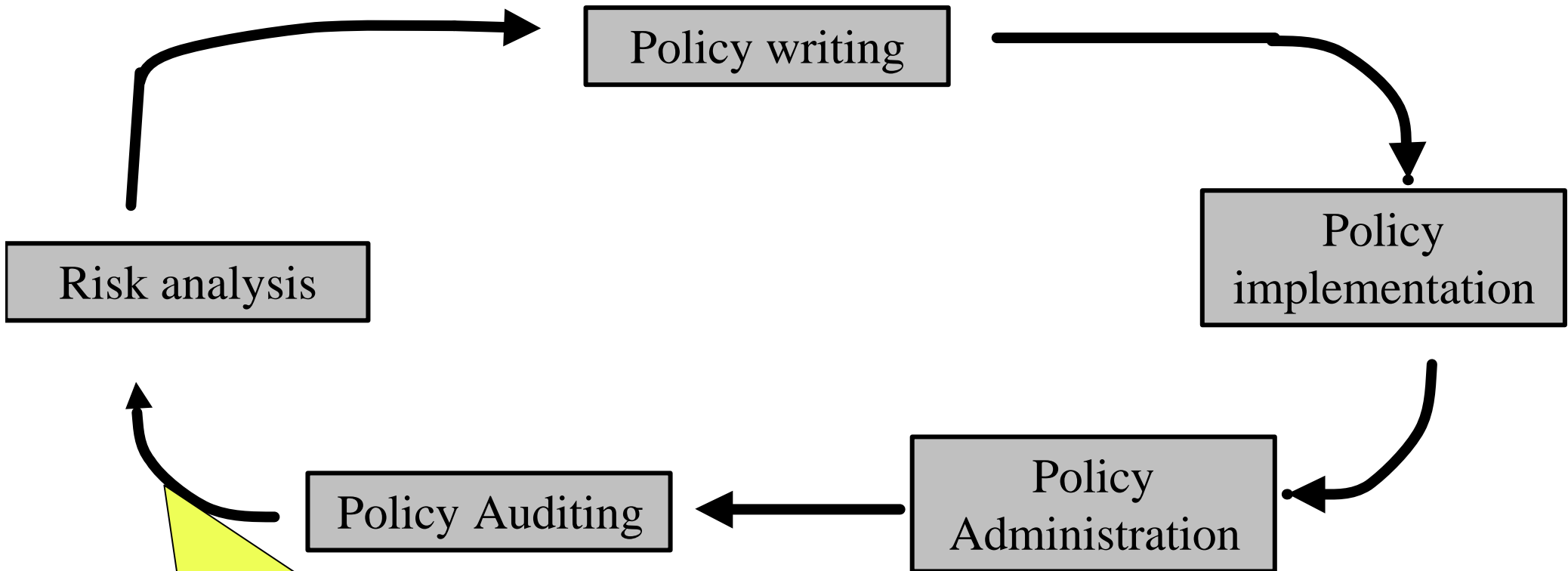
Security Incidents (% of respondents)	1999	2001	2003
	Unauthorized use of computer systems	62%	61%
Unauthorized access to www sites	20%	23%	25%
Total annual losses [\$]	\$136M	\$377M	\$201M**

\* 1998

\*\* only 47% of respondents could quantify financial loss

Source: Computer Crime & Security Survey, Computer Security Institute/Federal Bureau of Investigation, <http://www.gocsi.com>.

# An effective approach



- effectiveness (nr. of incidents, impact, ...)
- cost controls
- change in technologies
- ...

# Policy example

## Network use policy:

1. **Purpose** (the policy goal)
2. **Scope** (whom the policy applies to)
3. **Policy**
  - a. Acceptable protocols (http, ftp, ...)
  - b. E-mail use (attachments, content, ...)
  - c. Internet use (downloads, sites, ...)
  - d. Personal use (accepted, forbidden, only after 5pm, ...)
  - e. ...
4. **Enforcement** (consequences of violations)
5. **Definitions**
6. **Revision history**

# Policy example [cont.]

## Antivirus policy:

1. **Purpose** (the policy goal)
2. **Scope** (whom the policy applies to)
3. **Policy**
  - a. SW to be used
  - b. Scheduling
  - c. What to do in case of virus found
  - d. ...
4. **Enforcement** (consequences of violations)
5. **Definitions**
6. **Revision history**

# Policy example [cont.]

## Network Administrators policy (set of sub-policies):

1. **Purpose** (the policy goal)
2. **Scope** (whom the policy applies to)
3. **Policy**
  - a. Backup policy
  - b. Disaster Recovery policy
  - c. Incident Handling policy
  - d. Users policy (permissions, quotas, ...)
  - e. ...
4. **Enforcement** (consequences of violations)
5. **Definitions**
6. **Revision history**

# A few tips on developing security policies

- **Policies are the starting point**
- **Weakest link rule** (develop with man in mind)
- **Importance of standards** (somebody did it and it works, people know what to do, audit is easier, partnerships)
- **Develop at corporate level** (explain the why, not the how; show "business" importance)

# A few tips on developing security policies [cont.]

- **Keep out operational issues** (standards and procedures for that)
- **Make them easily accessible and available**
- **Audit, evaluate, change** (cicle)
- **One step at a time**

**Remember:** It takes time, it is hard, results will not come soon.

# Business vs. security

Never forget that **“business is the goal”**

- Security must enable and not deny
- Security must make things easier not harder
- Security requires efforts & investments
  
- ... Security gives results ... (business results)

# *“Advantages in defining and adopting a security policy”*

*Information & Network Security Workshop - Bologna, 1<sup>st</sup> July 2003*



**info@infosec.it**

**www.infosec.it**

**Speaker: Angelo Perniola - Infosec Project Manager  
perniola@infosec.it**