



**FIST Conference October 2003 @**



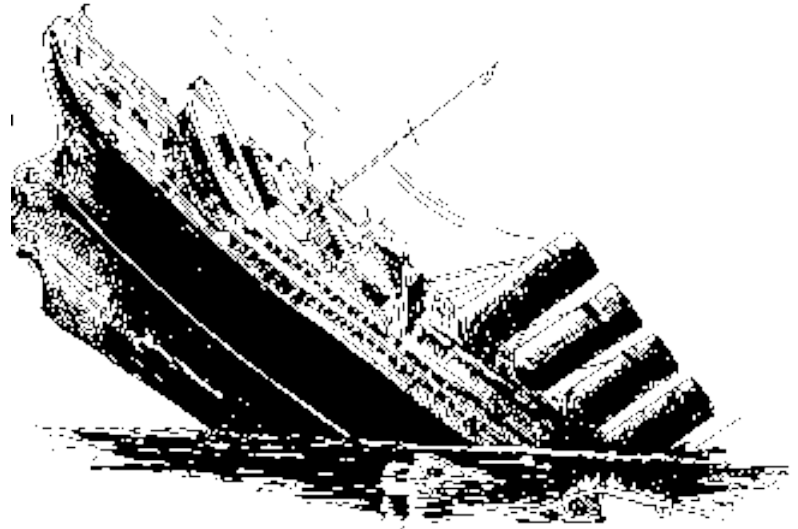
# **Return on Security Investment**

**© Vicente Aceituno**





# Why expend on security measures



Just one word: **INCIDENTS**



# The direct cost of incidents

**The direct cost of incidents is:**

**Income loss.**

**Property damage and loss.**

**Direct economic loss.**



**Plus the cost to return the system to the pre-incident state.**

**Other direct cost could be:**

**Human life.**

**Information loss.**

**Penalties.**



# The indirect cost of incidents

**Damaged Image.**

**Loss of Trust.**

**Treasury problems.**

**Breaching of contracts and other legal responsibilities.**

**Social and moral obligations breaching.**

**Additional costs.**





# Lifecycle of Information Systems

Requirements (Business, User, Technical, **Security**).

Analysis.

Design.

Construction.

Quality Assurance (Testing).

Implementation.



More often than not **security requirements** are not considered.



# Quality Assurance

**Testers** emulate **authorized users** performing  
Business Requirements Tests.  
User Requirements Tests.  
Technical Requirements Tests.  
Security Requirements Tests.



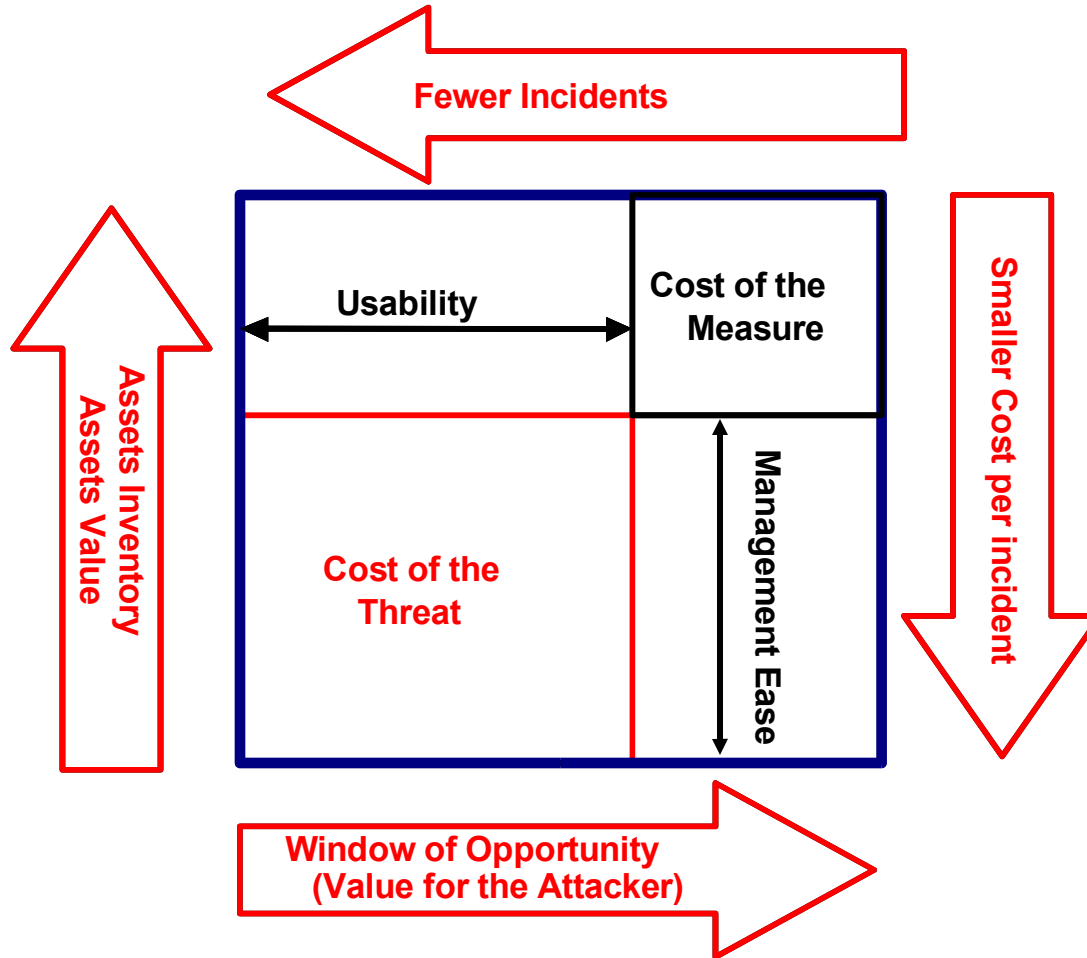
**PenTesters** emulate **unauthorized users** trying to overcome security measures.

**Auditors** mostly check existing evidence





# How to turn intuition into hard data?





# Widespread knowledge

## Mayfield's Paradox

It cost an infinite amount of money both to give everyone access to a system, and to prevent everyone access the same system.



## CMU – CERT study:

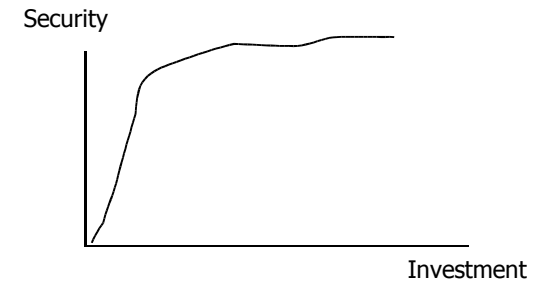
The more you spend, the less difference it makes on your security.

## Idaho University formula.

$$(R-E)+T= ALE$$

$$R-ALE=ROSI.$$

$ROSI=E-T$ , but where do you get E?



## Problem: Lack of real Data & too many assumptions:

Risk Cost monotonically decreases with investment.

Risk Cost is subject to diminishing return on investment.

ROSI is positive for all levels of investment.



# What is ROSI for?

**It's not about how much you make, it's about where do you put your budget!**

Nowadays, security measures are selected based on:

**Fear Uncertainty and Doubt decisions.**

**Paranoid decisions.**

**Coolness decisions.**

**Random decisions.**



**A ROSI based decision allows for:**

**Selecting the best security measures with a given budget.**

**Determine if a budget is enough to meet security targets.**

**No security measure is ever selected based on profitability.**



# Security Measures

There are two distinctive kinds of Security Measures.

Vulnerability reduction of **specific** risks. (aka Preventive)

Firewalls.

Locks.

Access Control.

...



Impact reduction of **unspecific** risks. (aka Paliative)

RAID.

Data Backup.

Redundant communications links.

...





# Vulnerability Reduction Security Measures Benefits

Vulnerability reduction means less incidents.

$$\text{ROSI} = (\text{RC}_{\text{before}} - \text{RC}_{\text{after}}) / \text{SM}_{\text{cost}}$$



When  $\text{ROSI} > 1$ , the security measure gives a return.

**RiskCost** = Number of Incidents\*Cost of an Incident. It depends strongly on the environment and number of potential targets.

You need hard data to calculate RC.To get hard data you need Information Gathering.

The security measure must prevent incidents for at least what it is worth per investment period.



# Vulnerability Reduction Measures ROI

## Example:

There are two laptop thefts out of 50 in a year.

A laptop replacement cost is 1800 euros.

The following year there are 75 laptops in the company.

60€ latches protect every laptop.

There is only 1 laptop theft the following, when the latches are installed.





# Vulnerability Reduction Measures ROI

$$ROSI = (RC_{\text{before}} - RC_{\text{after}}) / S_{m_{\text{cost}}}$$

$$ROSI = ((1800 + I_v) * 3 - ((1800 + I_v) * 1 + 75 * 60)) / (75 * 60), I_v = 0, ROSI < 1.$$

\*Incidents are adjusted for increased number of “targets”.

If a laptop’s information worth is nil, the security measure return is unprofitable.

For this example, 60€ latches give a return when any laptop’s Information value is over 2700€, or when you expect 5 thefts for this year (based on historic info).

With this kind of analysis, you could:

Decide to use latches only for laptops that hold valuable information.

Calculate the maximum you should pay for latches for all laptops (24€ when  $I_v = 0$ ).



# Impact Reduction Security Measures Benefits

**Impact reduction is like insurance: It puts a cap on your maximum loss.**

**You can't measure impact reduction investment return.**

**When the best happens it is never used. When the worst happens twice, it seems to be worth twice the value of your assets, but who would spend twice the worth of anything in security measures?**

**The real factor is what protection do you get for your money.**

**You can measure efficiency. For Time to Recover efficiency, you have off-site backups (some extra cost) on one end, and fully redundant systems (over 2X cost) on the other.**



**Ideally this security measures are never used.**



# Hard Data based Choices

	Direct cost	Indirect cost
<b>Vulnerability Reduction</b>	<b>Choice based on risk cost reduction</b> <b>ROSI &gt; 1</b>	<b>Quality Assurance:</b> <b>Penetration Testing.</b> <b>Auditing.</b> <b>Information Gathering from IDS, Honeypots, logs, etc.</b>
<b>Impact Reduction</b>	<b>Choice based on Efficiency</b> (“bang for the buck”, normally <b>Time to Recover</b> )	<b>Quality Assurance:</b> <b>Incidents Emulation.</b> <b>Forensics.</b> <b>Information Gathering from Incidents Evaluation.</b>
<b>Information System Lifecycle</b>	<b>Choice of Security Requirements</b>	<b>Quality Assurance:</b> <b>Security Requirements Testing.</b> <b>Code Auditing.</b>



# Afterthoughts.

**To take hard data based decisions you have to assume the indirect cost of information gathering.**

**Information systems designed with security requirements in mind are cheaper in the long run.**

**Your neighbour's security measure with the best ROSI won't necessarily be yours too.**

**Don't be tight: Use impact reduction measures for critical assets.**

**Assume testing and trial of your security measures as an indirect cost.**





# **Return on Security Investment**

## **FIST Conference**

**© Vicente Aceituno**

**25 October 2003**

