

# Rafizza Expertise, PT

## **Overview** **Information Security**

**<http://www.rafizza.com>**

**email:sbw@rafizza.com**

*Optimizing your business*

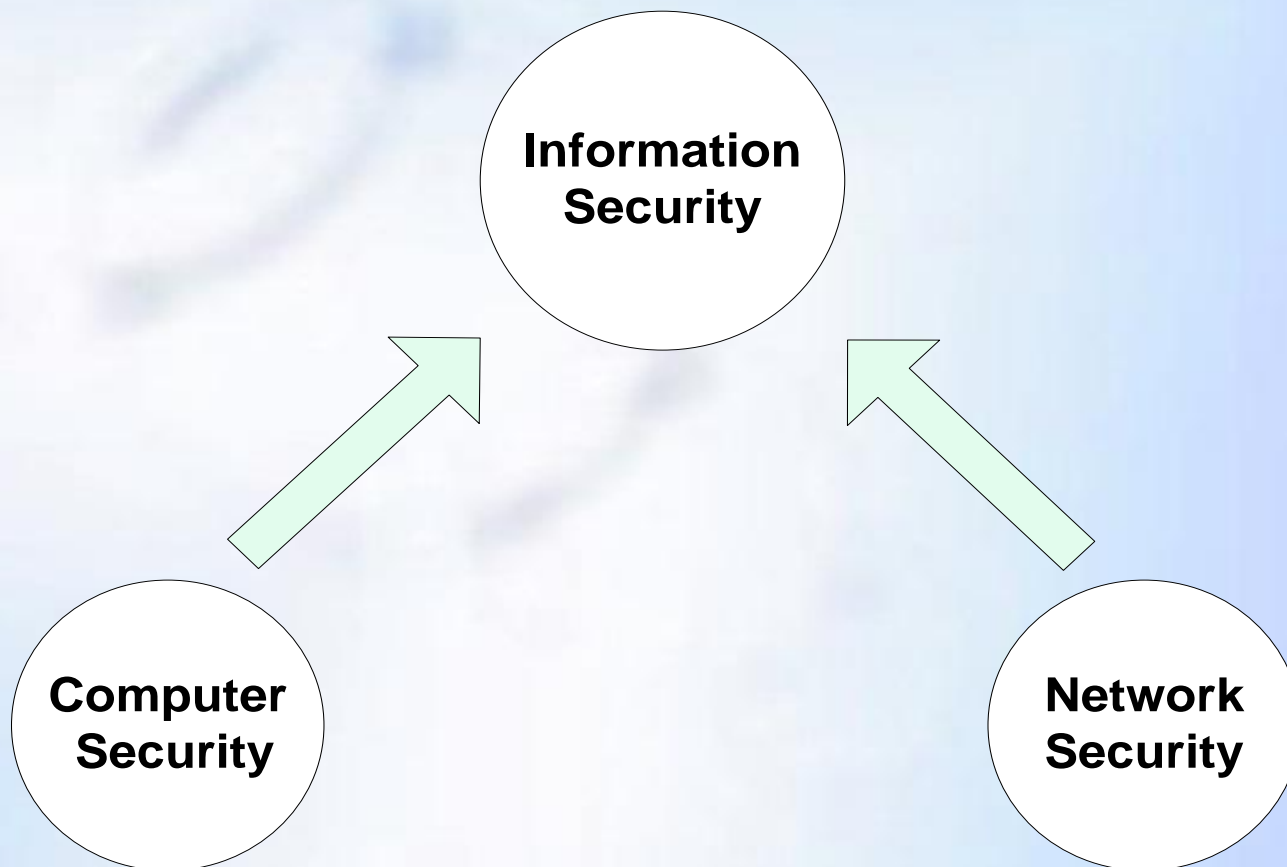
**RE** *Rafizza  
Expertise*

# Why ??

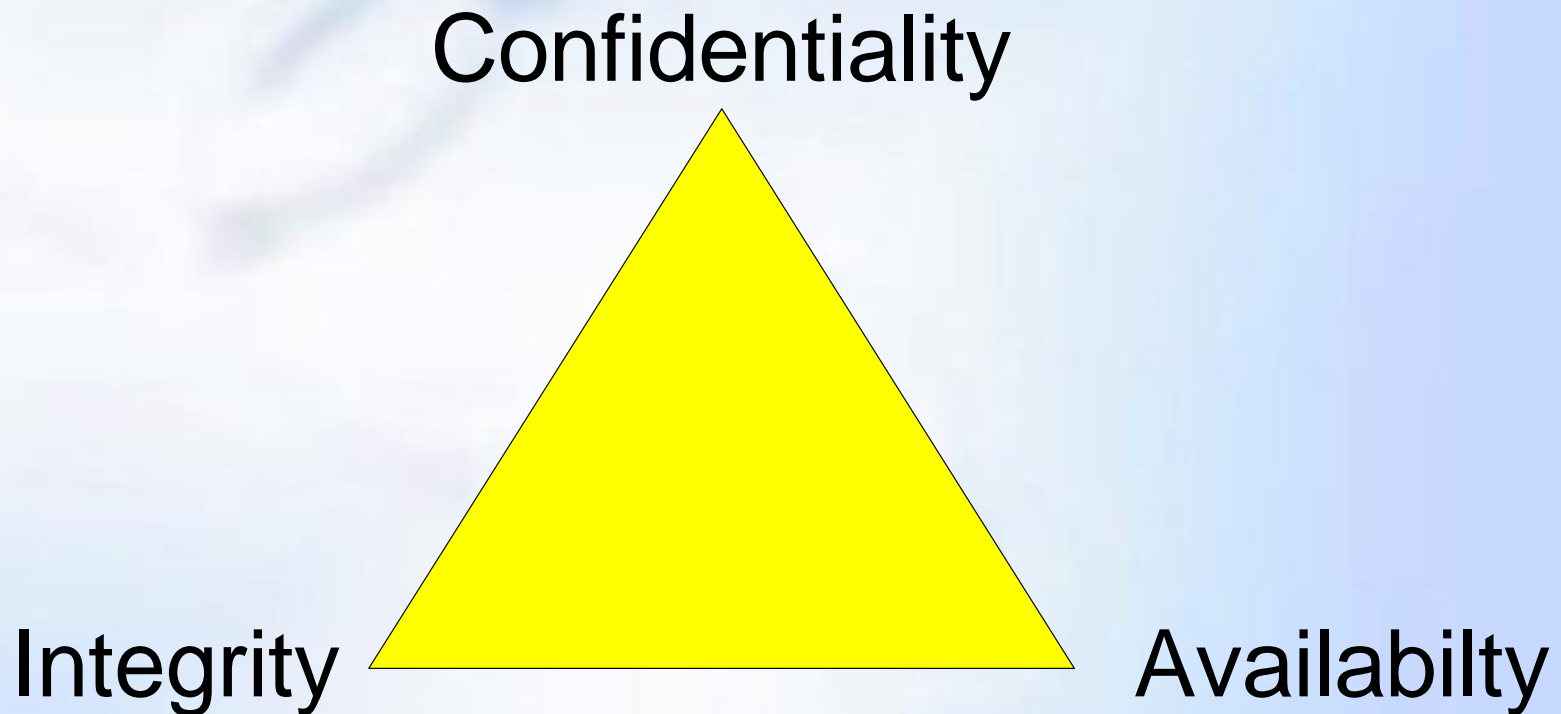
Why do we need to secure  
our Computer  
and Network ?



# Information Security



# Fundamental Principles (1)



# Fundamentals Principles (2)

- Confidentiality. The concept of confidentiality attempts to prevent the intentional or unintentional unauthorized disclosure of message's contents.
- Availability. The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate personnel

# Fundamentals Principles (3)

- Integrity. The concept of integrity ensures that :
  - Modifications are not made to data by unauthorized personnel or process.
  - Unauthorized modifications are not made to data by authorized personnel
  - The data internally and externally consistent

# Risk Management

Risk Management's main function is to mitigate risk. Mitigating risk means to reduce the risk until it reaches a level that is acceptable to an organization

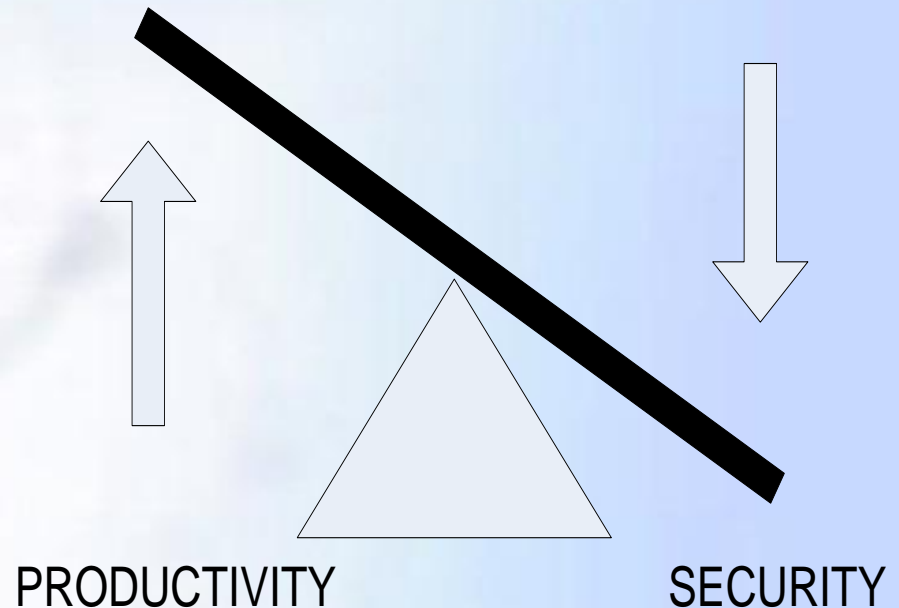
Risk Management consist of the following:

- Performing Risk Analysis
- Implementing, reviewing and maintaining

# Security vs Productivity (1)

## **Lack Of Security**

- High risk
- Low Cost
- Open access
- No productivity loss
- Open access may lead to data loss which may lead to productivity loss

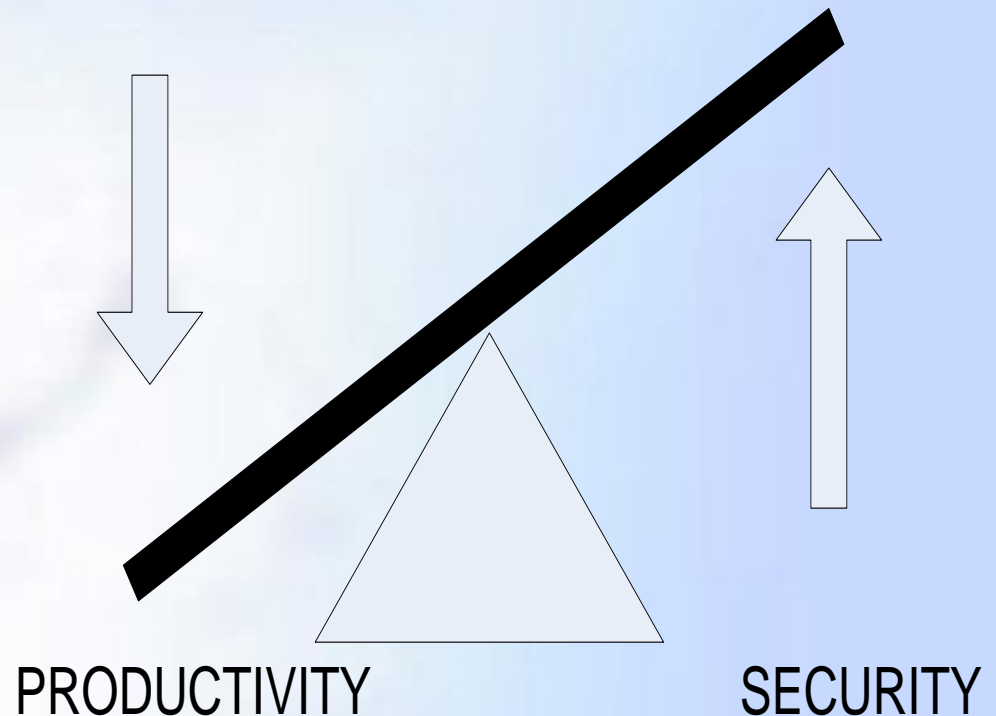




# Security vs Productivity (2)

## **Overly Restrictive Security**

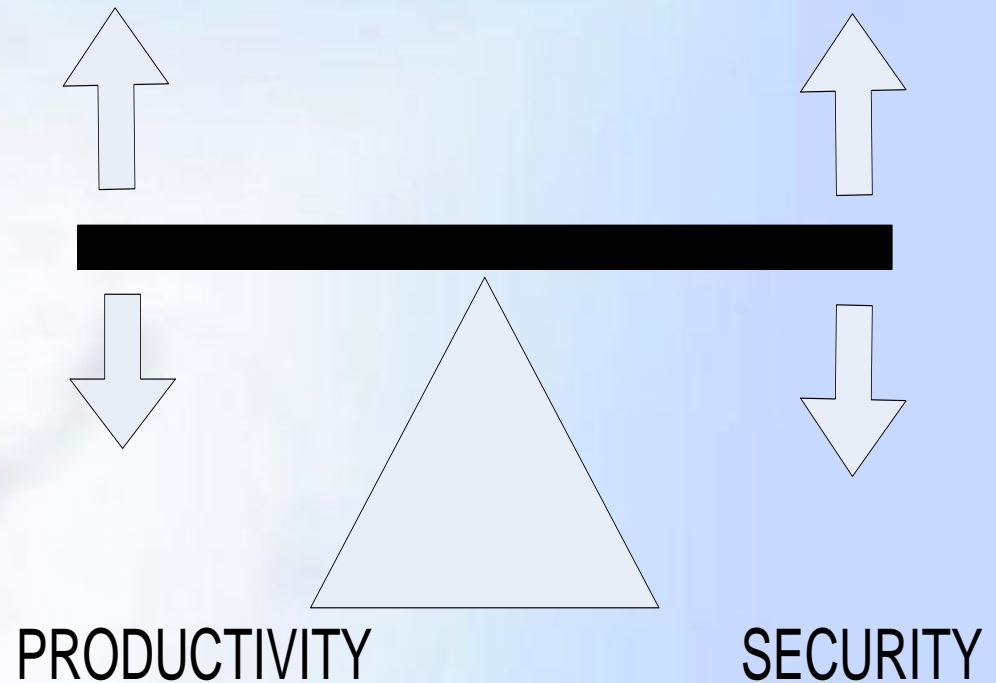
- High Cost
- Low Risk
- Productivity Loss
- Overly restrictive security may lead to noncompliance security process which may lead to loss of security



# Security vs Productivity (3)

## Optimal Balance

- Balance Risk and Cost
- Restrictiveness of security policy balanced by people's acceptance of those policies



# Security as a Process

- You cannot just rely on a single type of security to provide protection for an organization's information
- You cannot rely on single product

# Risk Analysis

The main purpose of performing a Risk Analysis is to quantify the impact of potential threats

## Risk Determination Table

No.	Asset	Threat	Vulnerability	Risk Level	Control

# Asset, Threat, Vulnerability, Control & Risk



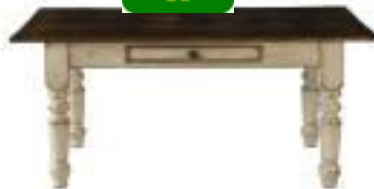
**Asset**



**Threat**



**Vulne-  
rability**



**Control**



**Risk**

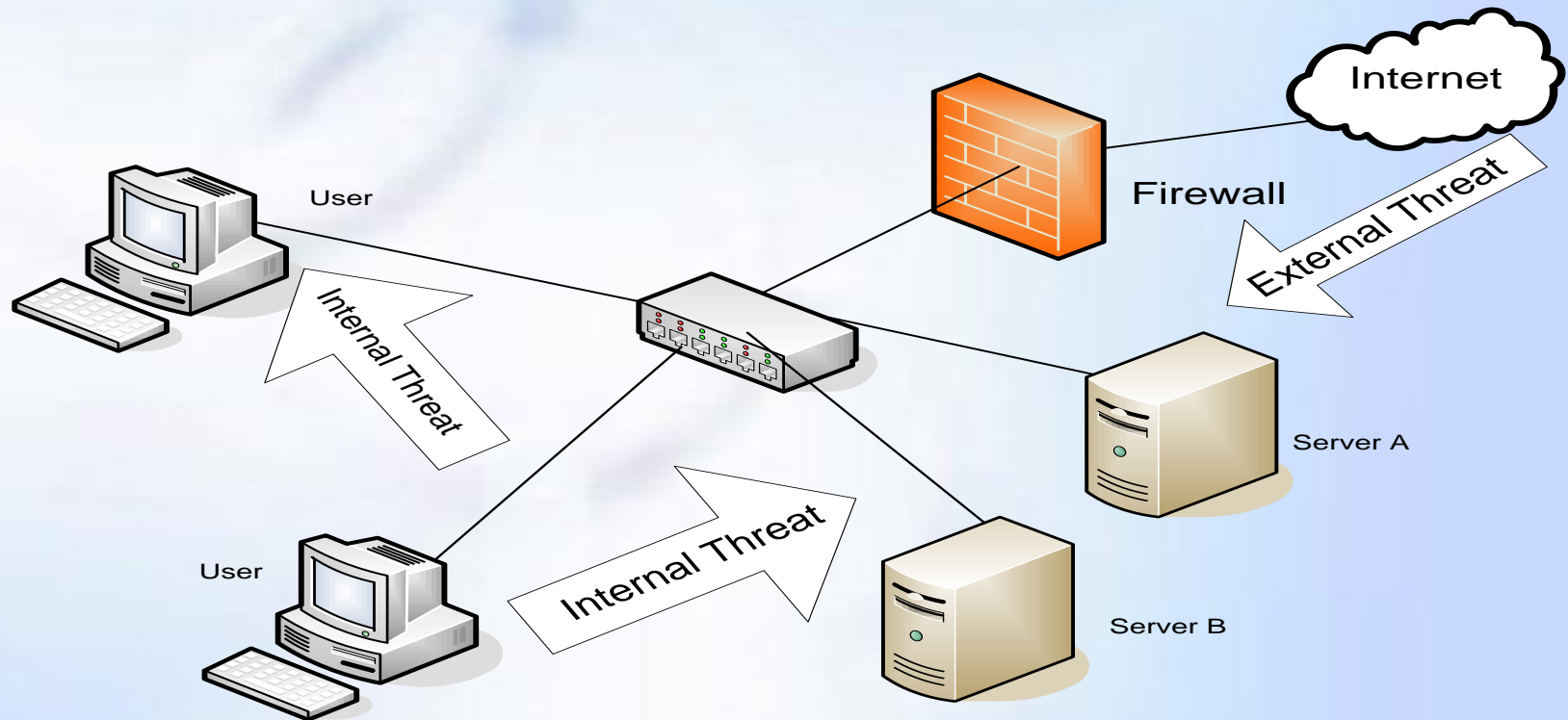
**Optimizing your business**

**RE** Rafizza <sup>13</sup>  
Expertise

# Asset, threat & Vulnerability

- Threat can be defined as the presence of any potential event that could cause harm by violating security
- Vulnerability is defined as a weakness in a system that enables security to be violated.
- Asset is considered anything that is computing resource or ability, such as hardware, software, data and personnel

# Internal & External Threat





# Controls

Controls are implemented to mitigate risk and reduce the potential loss

Controls can be preventive, detective and corrective.

Preventive controls are put in place to inhibit harmful occurrences

Detective controls are established to discover harmful occurrences

Corrective controls are used to restore system that are victims or harmful attacks



# Implementation Control

- Administrative control  
Policies, procedure, security awareness training and increase supervision
- Technical control  
Restriction of access to systems and the protection of information.
- Physical control  
Building security in general

# Control Combination

- Preventive / Administrative
- Preventive / Technical
- Preventive/ Physical
- Detective / Administrative
- Detective / Technical
- Detective / Physical

# Models for Controlling Access (1)

- Mandatory Access Control

The authorization of a subject's access to an object depends upon labels which indicate the subject's clearance and the classification or sensitivity of the object.

For Example unclassified, confidential, secret and top secret.

# Models for Controlling Access (2)

- Discretionary Access Control  
The subject has authority, within certain limitations, to specify what objects are accessible.
- Non-Discretionary Access Control  
A central authority determines what subject can have access to certain objects based on the organizational security policy.

# Identification & Authentication

Identification and authentication are the keystones of most access control systems.

Identification is the act of a user professing an identity to a system

Authentication is verification that the user's claimed identity is valid

# Security Technologies

- Firewalls
- Network Partitioning
- Virtual Private Networks
- Encryption
- Intrusion Detection System
- Anti-virus
- Anti-spyware

# Is it enough ?



**Control**



**Risk**



**Optimizing your business**

**RE** Rafizzø3  
Expertise



# Policy

- Policy provides the rules that govern how systems should be configured and employees with the corporation understand how to act
- Policy defines what security should be within organization
- Policy puts everyone on the same page so everyone understands what is expected



# Security Development Life Cycle

