



# Cost Estimation for Secure Software & Systems Workshop Introduction

Edward Colbert, Sr. Research Associate  
Dr. Barry Boehm, Director

Center for System & Software Engineering  
{ecolbert, boehm}@csse.usc.edu  
<http://csse.usc.edu>

Ground Station Architecture Workshop (GSA)



# Goal Of Presentation

## Review Research

- Draft model for early costing of **system** security
- Extensions to COCOMO II for development of secure software systems (“COSECMO”)

## Invite

- Expert opinion
- Data (Collection)



# U.S. Federal Aviation Administration Needs

- ❑ U.S. Congressional & Congressional Office of Management & Budget (OMB) requires each U.S. agency to **plan & budget for security** throughout life-cycle of system
  
- ❑ July '03, FAA CTO asked USC CSSE to research cost estimation for secure systems
  - Completing 3<sup>rd</sup> phase



# Estimating Cost for Secure Software-Intensive Systems

- ❑ Widely held that engineering security will substantially raise software-project cost
- ❑ Wide variation in amount of added cost estimated by different models
  - e.g.
    - [Bisignani and Reed 1988] estimates engineering highly-secure software will increase costs by **factor of 8**
    - 1990's Softcost-R model estimates **factor of 3.43** [Reifer 2002]
- ❑ Models based on 1985 “Orange Book”
  - *DoD Standard 5200.28-STD, Trusted Computer System Evaluation Criteria* [National Computer Security Center 1985]

EC1

**Slide 4**

---

**EC1**

**Name & reference**

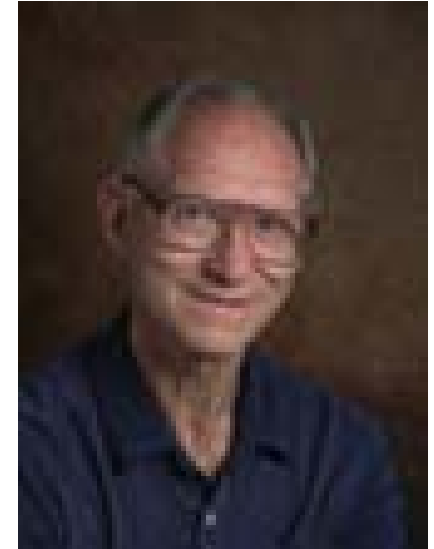
Ed Colbert, 12/7/2005

# Estimating Software Cost

- ❑ 1981 *Constructive Cost Model (COCOMO)*
  - 80 projects
  - Developed by Dr. Barry Boehm
  
- ❑ 2000 COCOMO II
  - 160+ projects
    - (now about 200 in database)
  - Authors
    - Dr. Boehm (USC CSSE)
    - A. Winsor Brown (USC CSSE)
    - Dr. Chris Abts (Univ. of Texas) \*
    - Dr. Sunita Chulani (IBM)\*
    - Dr. Brad Clark (Software Metrics, Inc.)\*
    - Dr. Elis Horowitz (USC CSSE)
    - Dr. Ray Madachy (CostPlus, USC CSSE)\*
    - Don Reifer (Reifer Consultants, Inc.)
    - Dr. Bert Steece (USC Marshall School of Business)

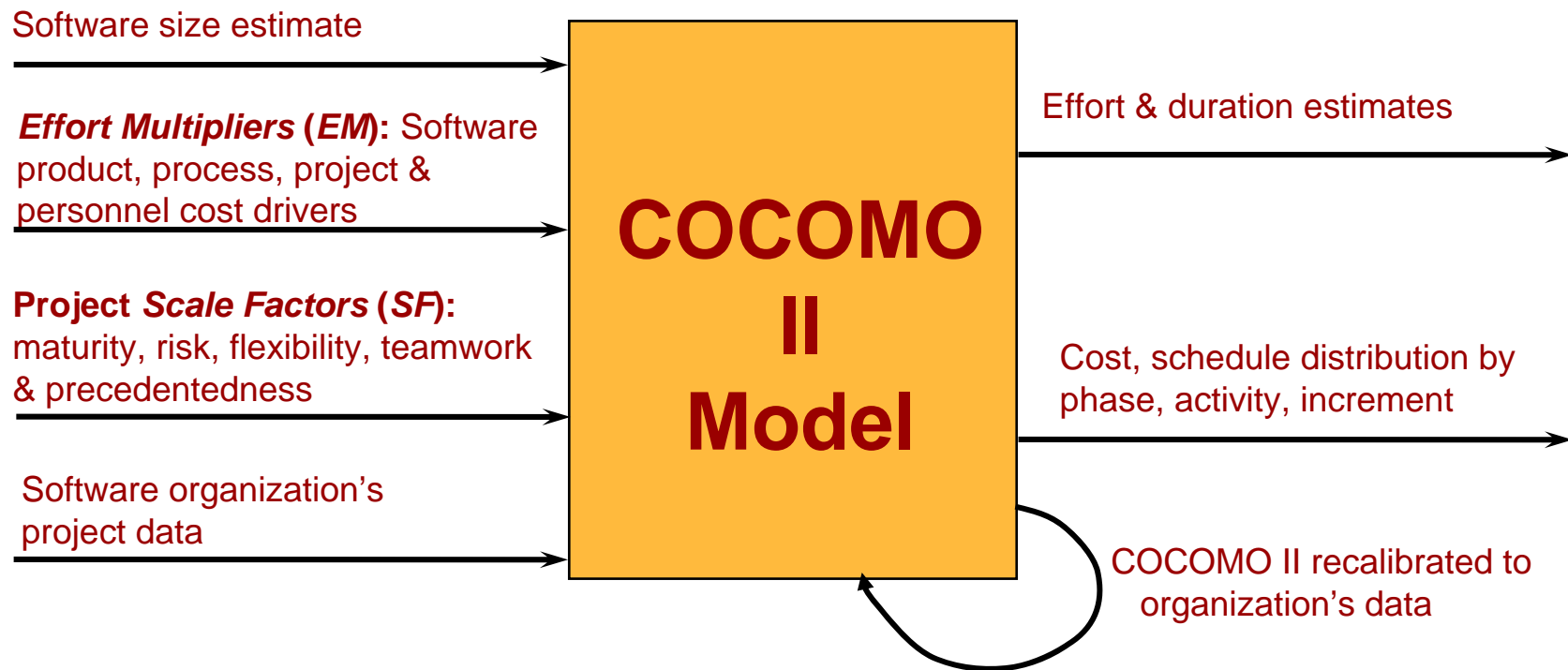
\* Dr. Boehm's Ph.D. Student

- ❑ COCOMO I/II is basis of many commercial products



- ❑ Dr. Barry Boehm
  - Director, USC Center for Software Engineering (USC CSSE)
  - Author of *Software Engineering Economics*
    - Seminal work on topic
  - Lead author of *Software Cost Estimation and COCOMO II*
  - Creator of *Spiral Model*
  - Former Director of Defense Advanced Research Product Agency (DARPA) Information Science & Technology Office

# COCOMO II & Security

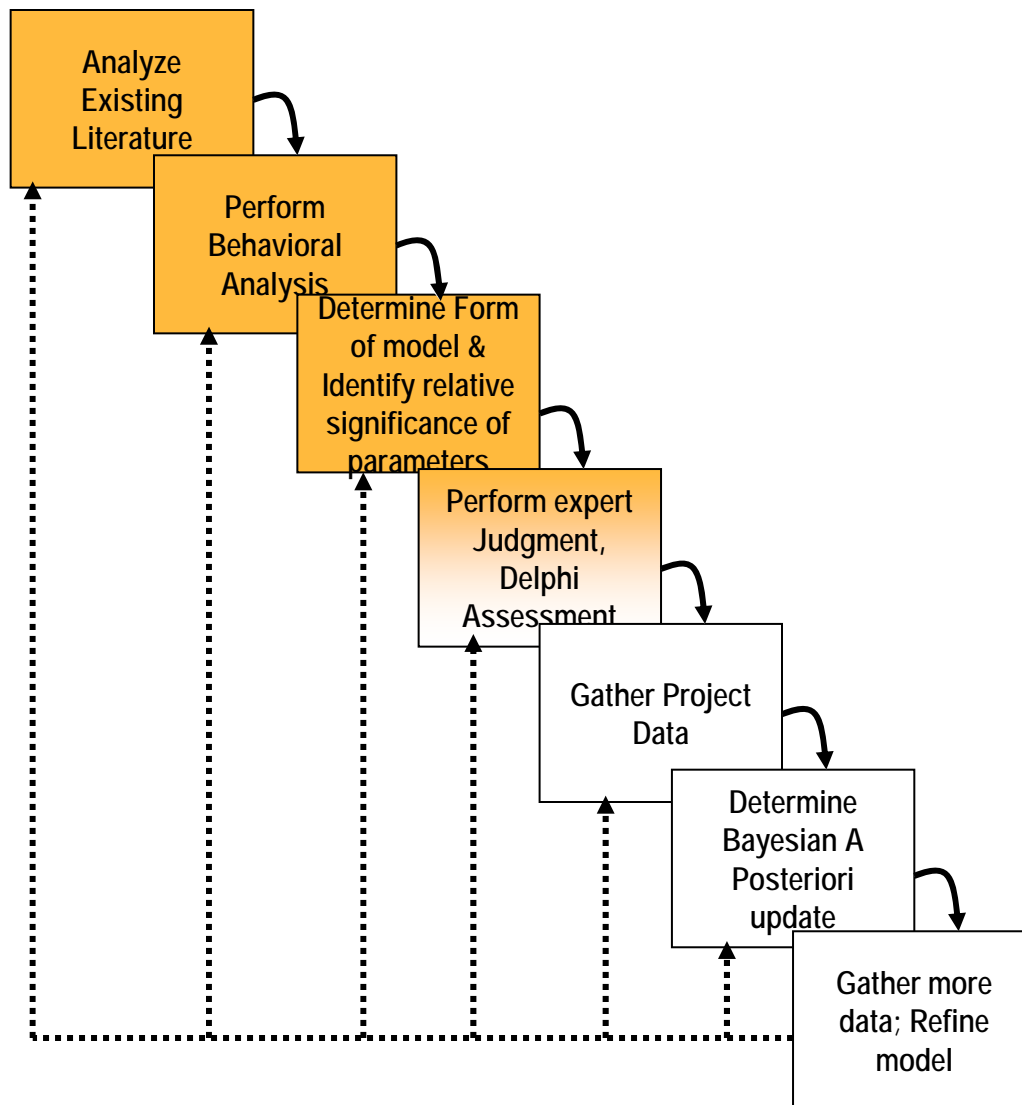


## Effort in Person Month

$$E_{base-estimate} = A * (Size)^S * \Pi(EM_i)$$

$$S = B + 0.01 * \Sigma(SFi)$$

# COCOMO II Modeling Methodology



## □ Analyzed

- Published industry practices with respect to security inc. standards like *Common Criteria*
- 149 Security Targets registered on National Information Assurance Partnership (NIAP) Website
  - SAR's & FAR Usage
    - Overall
    - By
      - » Project Domain
      - » Life-cycle phase
      - » Security goals
      - » COCOMO driver

## □ Conducted preliminary surveys of experts in SW development & in security





# COCOMO Estimation with Security

$$\begin{aligned} \%Effort(EAL) &= \%Effort_3 * SECU^{(EAL - 3)} && \text{for } EAL \geq 3 \\ &= 0 && \text{for } EAL < 3 \end{aligned}$$

$$Effort(\text{Internal Assurance}) = Effort(\text{Base}) * \%Effort(EAL)$$

$$\begin{aligned} Effort(\text{Total}) &= Effort(\text{Base}) + Effort(\text{Internal Assurance}) \\ &\quad + Effort(\text{Independent Assurance}) \end{aligned}$$

where:

- |                               |   |
|-------------------------------|---|
| SECU                          | — Calibration constant  |
| EAL                           | — Evaluated Assurance Level or (Equivalent)   |
| Effort(Base)                  | — Result from basic COCOMO II formula   |
| Effort(Internal Assurance)    | — Effort of developer to verify that security requirements are met                          |
| $\%Effort_3$                  | — Percent add effort at level 3 (see table next page)                                       |
| $\%Added\ Effort$             | — Percent added effort for desired AL   |
| Effort(Independent Assurance) | — Effort of independent organization's effort to verify that security requirements are met. |

# COCOMO Estimation with Security (cont.)

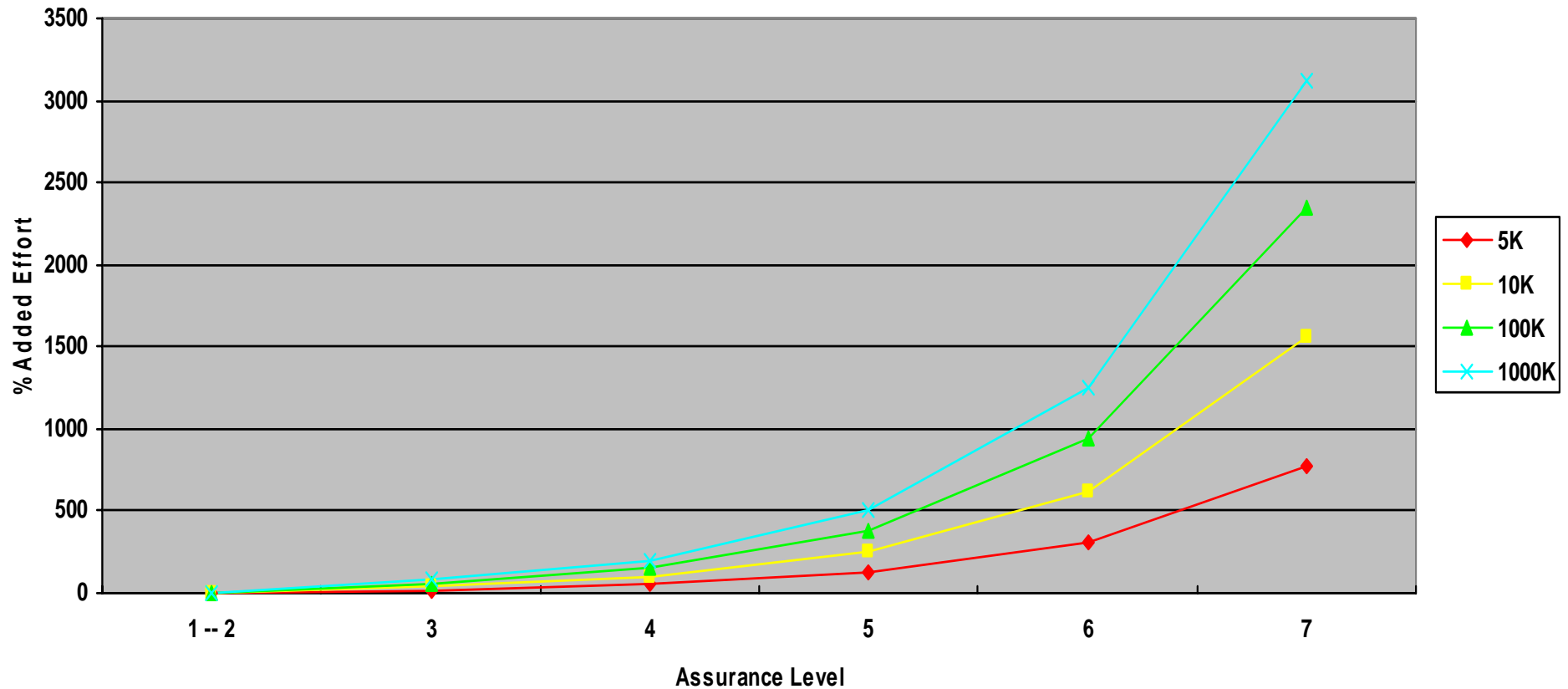
## %Added Effort when SECU = 2.5

System Size (KSLOCS)	Assurance Level					
	Nominal	High	Very-High	Extremely-High	Super-High	Ultra-High
5	0	20	50	125	312	781
10	0	40	100	250	625	1560
100	0	60	150	375	937	2344
1000	0	80	200	500	1250	3125

- Level names are COCOMO standard + 2
  - Mapping currently from Common Criteria v2
    - Nominal=1 or 2, High=3, Ultra=7
    - For 3+, Reliability = Very-High
  - Working on other mappings (e.g. NIST 800-52, DoD 8500, Orange Book)
- Values are based on survey of small group of experts
- Published data points fit reasonably
  - Only a few data points

# COCOMO Estimation with Security (cont.)

## %Added Effort



What's your opinion?



# Example of COCOMO Estimation with Security

## Assume:

Reliability = Very-High

All other drivers = Nominal

Trusted SW = 5 KSLOC

If Assurance = Nominal (EAL 1 or 2)

Effort(Total) = 21.75 person-months

If Assurance = Very-High (EAL 4)

Effort(Internal Assurance) =  $21.75 * 50\%$  = 10.88 person-months

Effort(Total) =  $21.75 + 10.88$  = 32.63 person-months

If Assurance = Ultra-High (EAL 7)

Effort(Internal Assurance) =  $21.75 * 780\%$  = 169.62 person-months

Effort(Total) =  $21.75 + 10.88$  = 191.37 person-months



# Formula for Cost of System & Security

$$C_{\text{total}} = C_{\text{Initial/Mission Analysis}} + C_{\text{Investment Analysis}} + C_{\text{System Engineering}} + C_{\text{Dev \& Imp}} + C_{\text{Sys of Sys Integration}} + C_{\text{Install/Deployment}} + C_{\text{O\&M}} + C_{\text{Disposal}}$$

$$C_{\text{Dev \& Imp}} = C_{\text{Design \& Build HW}} + C_{\text{Design \& Build SW}} + C_{\text{Purchased Services}} + C_{\text{COTS-Sys}} + C_{\text{Env-Mods-design}} + C_{\text{Bus-Proc-Re-engineering}}$$

$$C_{\text{total}} (\text{Security}) = C_{\text{total}} (\text{with security}) - C_{\text{total}} (\text{without security})$$

C = Cost



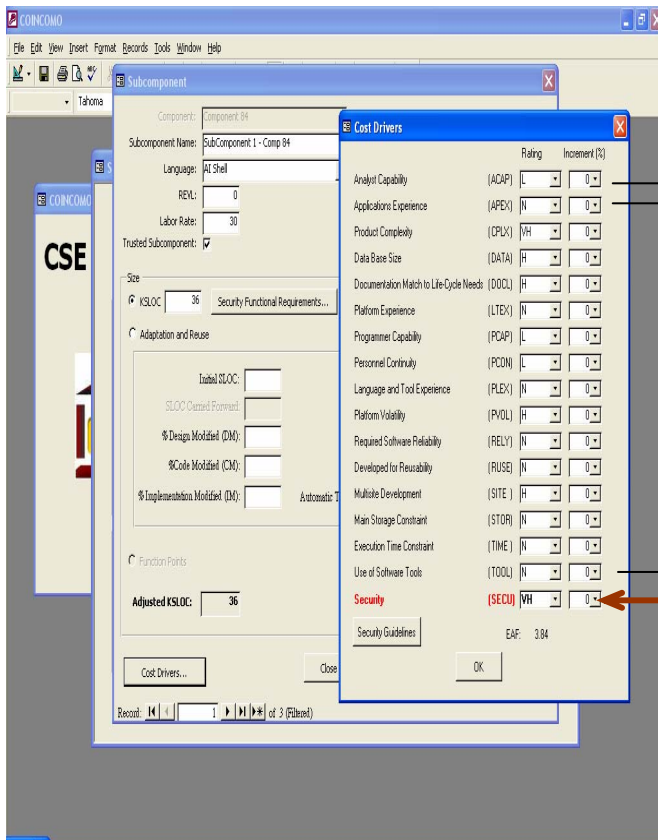
# Cost Model for Secure System Approach

- ❑ Analyzed Work-breakdown Structure (WBS)
  - Identified activities affected by Security
- ❑ Identified major sources of cost
  - To develop & own system
  - Including: facilities, equipment, people, acquired systems, services
- ❑ Determine approaches to estimate cost for each source of cost
  - Activity-based (e.g. Labor hours)
  - Unit costing (e.g. # firewalls)
  - Analogy-based (e.g. It cost us \$XXX last year,...)
  - Parametric (e.g. COCOMO II estimate)

# Developed Prototype Tool Support

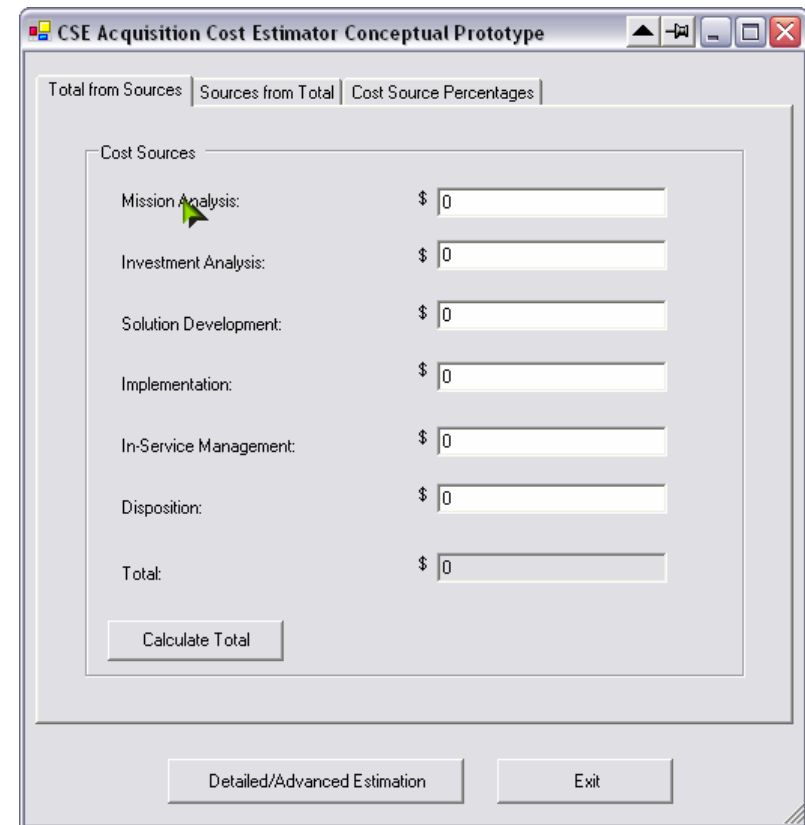
❑ COSECMO Prototype in COINCOMO

❑ 4th Prototype Tool Screenshot#1 Total from Cost Sources



Current COCOMO II Cost Drivers

Security Assurance Level





## To Do

- Get more feedback from security community
- Refine models
- Refine costing prototypes
- Refine Delphi
- Collect & analyze data
- Write papers & Ph.D. thesis (theses?)





# Next Costing Secure Systems Workshop

- Date: TBD June
  - Also, workshop at fall COCOMO Forum
- Location: University of Southern California, LA
- Cost:
  - TBD (nominal)

# In Case You Aren't Sure That Security Is Important





# References

- ❑ Bisignani, M. and Reed, T. (1988). "Software Security Costing Issues", *COCOMO Users' Group Meeting Proceedings*. Los Angeles: USC Center for Software Engineering.
- ❑ Boehm, B. W. (1981). *Software Engineering Economics*, Prentice–Hall: Englewood Cliffs, NJ
- ❑ Boehm, B. W. (1988). "A Spiral Model of Software Development and Enhancement", *IEEE Computer*. Vol. 21, No. 5 (May): pp. 61–72.
- ❑ Boehm, B. W. (1993). "A Spiral Model of Software Development and Enhancement", *Software Management*, D. J. Reifer ed., Fourth ed., IEEE Computer Society Press: Los Alamitos, CA. p. 120-131
- ❑ Boehm, B. W., Abts, C., et al. (2000). *Software Cost Estimation with COCOMO II*, Prentice–Hall: Englewood Cliffs, NJ
- ❑ National Computer Security Center (1985). *Trusted Computer System Evaluation Criteria* ("Orange Book"), Washington, D.C.
- ❑ Reifer, D. (2002). *Security: A Rating Concept for COCOMO II*. Reifer Consultants, Inc.