
# CSSPAB Workshop on "Approaches to Measuring Security"

## QUANTITATIVE RISK ASSESSMENT

Fred Tompkins

June 13, 2000

# AGENDA

- **OBSERVATIONS/ BACKGROUND**
- **RISK MANAGEMENT ANALYTICAL PROCESS**
- **RISK ANALYSIS**
- **RISK REDUCTION ANALYSIS**
- **SUMMARY**

# OBSERVATIONS

## “The Way We Think Is At Least As Important As What We Think”

**Owen Barfield**

# BACKGROUND

"The only certainty in life is death; uncertainty lies in when and how death occurs and whether it is final. Man strives to delay its onset and extend the quality of life in the interim. Threats to these objectives involve risks, some natural, some man-made, some beyond our control, and some controllable."

Thomas D. Rowe, "An Anatomy of Risk"

# Reality
## *In the Commercial Sector*

- **The "Now" Problem**
  - **COTS**
  - **Rate of Technology Change**
  - **Speed of Business**
  - **Risk Management**

# Industry Planning Time Frames

- Strategic Planning
- Tactical Planning
- Operational Planning

- 8-10 Months (old 3-5 yrs)
- 30 Days (old 1-3 yrs)
- 48-96 Hours (old 1 mo - 1 yrs)

# BACKGROUND

- "Organization and Business Case Model for Information Security" – Office of the Manager, National Communication System – 26 August 1997
  - Purpose: To develop a business based approach/methodology for justifying funding for information systems and network security expenditures
  - Hypothesis: Significant security incidents have provided motivation for security investments and that reasonable proactive security investment would have mitigated the effects of the incident, resulting in lower overall costs.
    - Research did not support the hypothesis
    - Organizations react to a variety of motivations for security investments; not just return on investment
    - Significant investments (generally over $1million) are subject to the rigors of a business case justification (as are all other significant investments).

Contact: Fred Herr, OMNCS

# BACKGROUND

- Industry Investment Today
  - **Industry typically spends 2-5% of IT budget on IA**
  - **Depends on industry sector**
  - **A lot of money in a $ trillion market**
- Future
  - **About 10% of new system investments**
  - **About 3-5% of operations budgets**

# RISK MANAGEMENT ANALYTICAL PROCESS

- **Risk Analysis**
- **Risk Reduction Analysis**
- **Management Decision**
- **Risk Reduction Plan**
- **Develop, Procure, Test, Implement**
- **Review and Audit**

# RISK ANALYSIS

- What's at Risk
- What are the Bad Things that can happen to what's at risk
- What is the likelihood that the Bad Things will happen
- What are the impacts/consequences if the Bad things happen

# RISK ANALYSIS

- **Threats**
- **Vulnerabilities**
- **Safeguards**
- **Expected/Anticipated Loss**

# CONTENTIOUS AREAS

- Value of Information
- Threat Likelihood
- Threat Frequency

**Any prediction about future events is highly subjective!**
**and, past performance is no guarantee of future performance.**

**At best, we can only hope to bound the likelihood and frequency of uncertainty.**

# RISK REDUCTION ANALYSIS

- **What's available to mitigate Vulnerabilities?**
- **Will they work in the environment?**
- **Are they cost effective?**

# RISK REDUCTION ANALYSIS

- **Technical Feasibility Analysis**
- **Operational Feasibility Analysis**
- **Economic Feasibility Analysis**

# SUMMARY

- **There are no Absolutes in dealing with future events**
- **In the end, we have to make decisions in the face of uncertainty**
- **Quantitative assessment of risk is a reasonable approach for getting close enough**

# CONTACT INFORMATION

**Fred Tompkins**

**COO/SR VP**

**Key Technologies & Security, Inc. (KTSI)**

**10688 Crestwood Drive, Suite B**

**Manassas, VA 20109**

**703.330.7117**

**ftompkins@ktsi.net**