

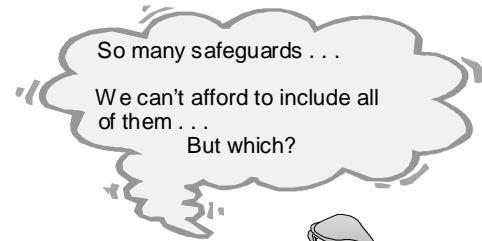
Risk Analysis and Security Design Methods

Richard Baskerville



1

Security Design Context of Risk Analysis



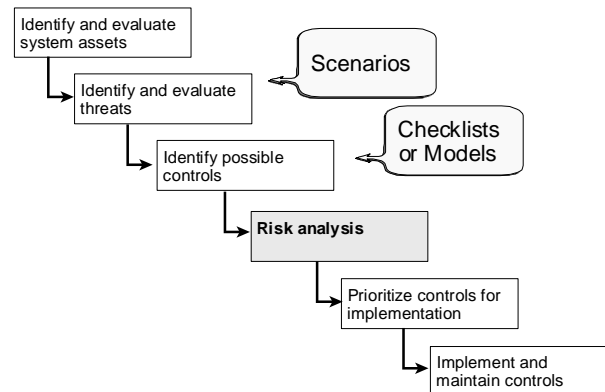
2

Quantitative Risk Analysis

3

Generic Security Design Model

Second Generation Methods



4

FIPS Pub 65

$$R = P \cdot C$$

Probability Range Table

	P
1/3 Years	0.33
1/30 Years	0.033
1/300 Years	0.0033
1/3000 Years	0.00033

Cost/Loss Range Table

	C
\$0 - \$1000	1000
\$1000 - \$10000	10000
\$10000 - \$100000	100000
\$100000 - \$1000000	1000000

Computer-based risk engineering

- P Interactive questionnaires
- P Threats database
- P Controls database
- P Analytic model



Riskpac Automated Process

Question File
Fraud #1
Fraud #2
Fraud #3

Responses to questions are summarized and related to risk profiles

Profile Table
Fraud profile X
Fraud profile Y
Fraud profile Z

Map file relates the selected risk profile to controls in the safeguards file

Standards File
S1: password policy
S2: compilation policy

Map File
X ∈ S1 & 2

Disk Crash Risk Exercise

Bayesian complexity: probability, risk and uncertainty

Statistical decision theory has developed a sophisticated body of thought that regards decisions about future (predicted) events. Their language carefully delineates the element of probability from risk (the random variation of the estimate from the actual) and from uncertainty (the error-induced variation of the estimate from the actual -- bad guesses) [DeGarmo, *et al*, *Engineering Economy* 1979].

9

The risk decision is interactive

- P The risk taker
- P The risk setting
- P Internal risk variability
- P The other risks

10

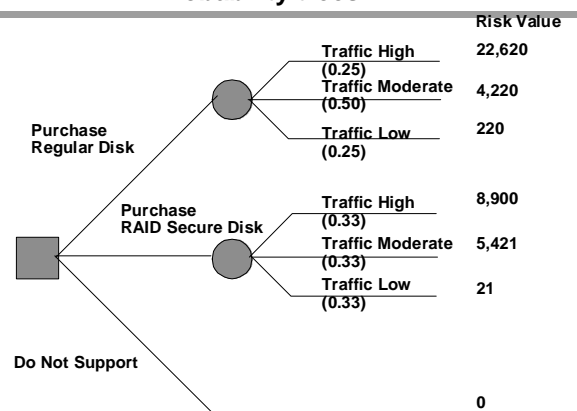
Risk adverseness

P Financial Concept of Risk - measure of the degree of variability of the outcomes over time

P Risk adverseness in decision makers - individuals sensitive to risk, utility curves

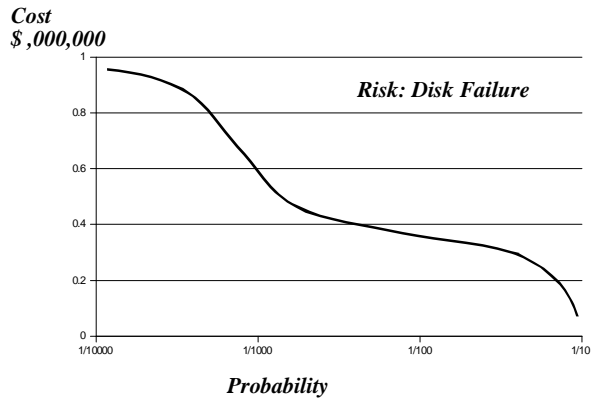
11

Probability trees



12

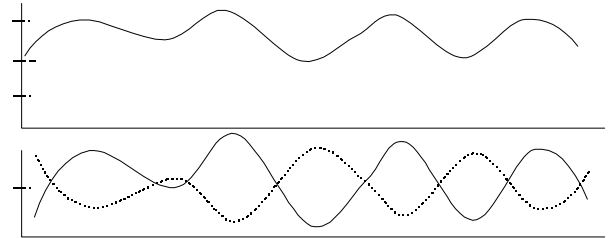
Risk curves



13

Portfolio theory

Diversification & relationship between the pattern of cash flows



14

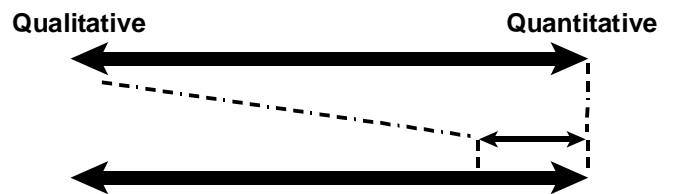
Is information security risk a quantitative issue?

15

Beware of the security quantoid-quantoid debate

P Scalar variables versus fuzzy sets

P Ratio versus ordinal or interval scales



16

Risk analysis controversy

P Authors' pet, practitioners' pariah?

P Problematic data collection

- Confidentiality
- Ambiguity
- "Dark figure" folklore

P Weak statistical model

P Irrefutable findings

P Ethics of monetary units & security "options"

17

Risk benefits and safeguards costs

18

Risk management methodology

P $V_{sc} = P \cdot D$

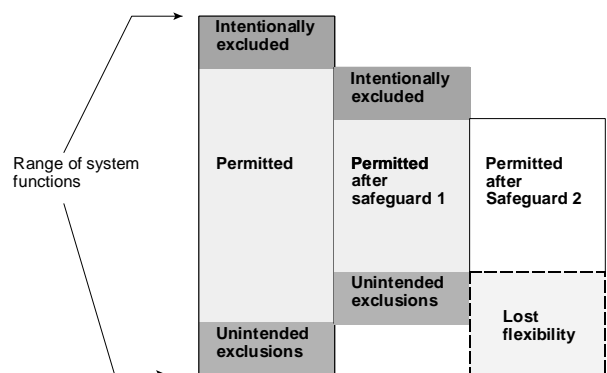
Value of a safeguard is a factor of the probability of a loss and the damage in the loss.

P $V_{sc} \geq C_{sc}$

Value of a safeguard must be greater than (or equal to) the costs of the safeguard

19

Safeguards constraining flexibility



20

Safeguard costs include

- P Simple implementation costs
- P Present value of the additional overhead
- P Present value of lost system benefits
- P Present value of lost system or security benefits
- P Present value of lost organizational opportunities

21

Scientific versus linguistic risk analysis

- P Analytic versus communicative artifacts
- P Interpretive, idiographic data points
- P Broad, interpretive statistic model
- P Situational findings

22

Linguistic risk analysis benefits

- P Reflects practitioner experience
- P Singular and particular
- P Concise communication channel
- P Formulated recommendations (explanation of method)

23

Risk analysis pitfalls

- P Inexperienced practitioners
 - Computer packages as replacements for experts
- P Generalizing data points
 - Similarity of risk profiles
- P Factoring the statistical model
 - Bayesian improvements

24

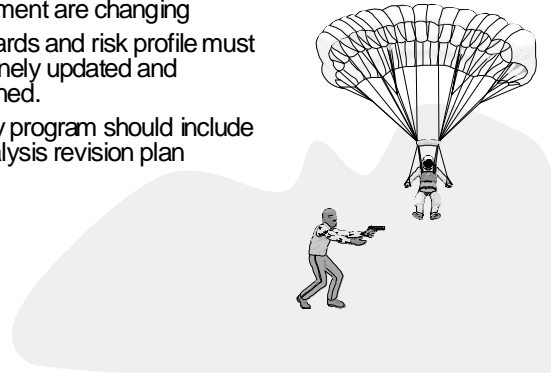
Risk analysis ethics

- P Results are expressed in monetary units
- P Admits that security is a capital investment opportunity
- P Defers security "option" to higher authority

25

Shifting Risk Profile

- P The organization and its environment are changing
- P Safeguards and risk profile must be routinely updated and maintained.
- P Security program should include risk analysis revision plan



26

27