Information Security Strategy: A short summary

Vincent LeVeque

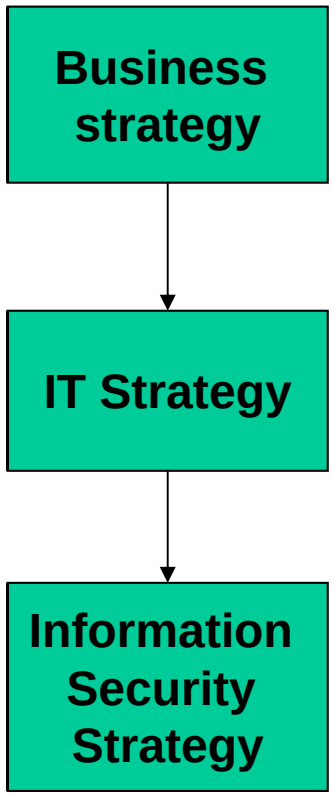
SAIC

vincent.e.leveque@saic.com

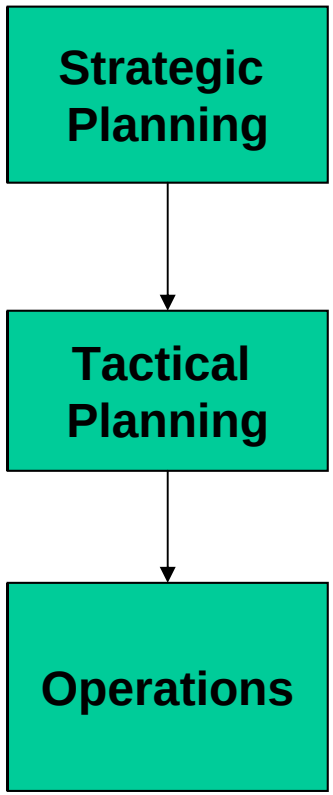
What is strategy?

- A long term plan
- Guides shorter term “tactical” plans
- Key to the organization’s mission
- Sometimes a formal planning methodology
- From the Greek strategos, a military leader

Where does “security strategy” fit in?



Where does “security strategy” fit in?



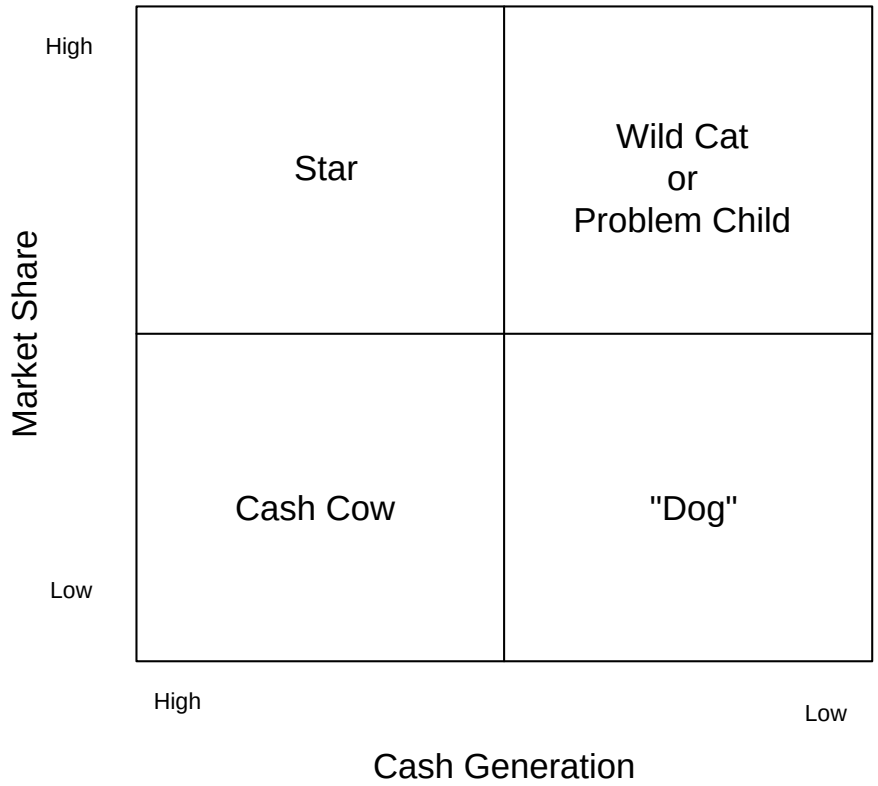
Models of business strategy

- Formal methods of analyzing the relationship between a mission, external forces, and internal strengths/weaknesses
- Examples:
  - The “Boston Square”
  - Competitive Advantage

The Boston Square

- Lifecycle based
- Driven by financial considerations
  - Growth
  - Cash flow
- Based on portfolio management

Boston Square



Competitive Advantage

- Competitive advantage = source of sustained profit advantage within industry
- Firm's relationship with suppliers, customers and competitors determines opportunities and threats
- How the firm deals with these opportunities and threats is categorized as a generic strategy
- The generic strategy should drive strategic planning

Models of IT strategy

- Nolan/Gibson Stages of Growth
- "Technocratic" strategy models
  - Information Engineering
  - Critical Success Factors
  - IBM's Business Systems Planning
- "Strategic Systems"
  - Can systems drive business strategy (rather than vice-versa)?

Nolan/Gibson Stages of Growth

- A life cycle approach, tying together technology expenditures, IT management styles, and technical infrastructure
- Proposed a natural evolution in the use and management of technology, driven by the problems of the prior stage

Nolan/Gibson Stages of Growth

- Stages:
  - Initiation
  - Contagion (unplanned growth)
  - Control
  - Integration (with broader business objectives)
  - Data Administration (organization-wide information sharing)
  - Maturity (full integration with business planning)

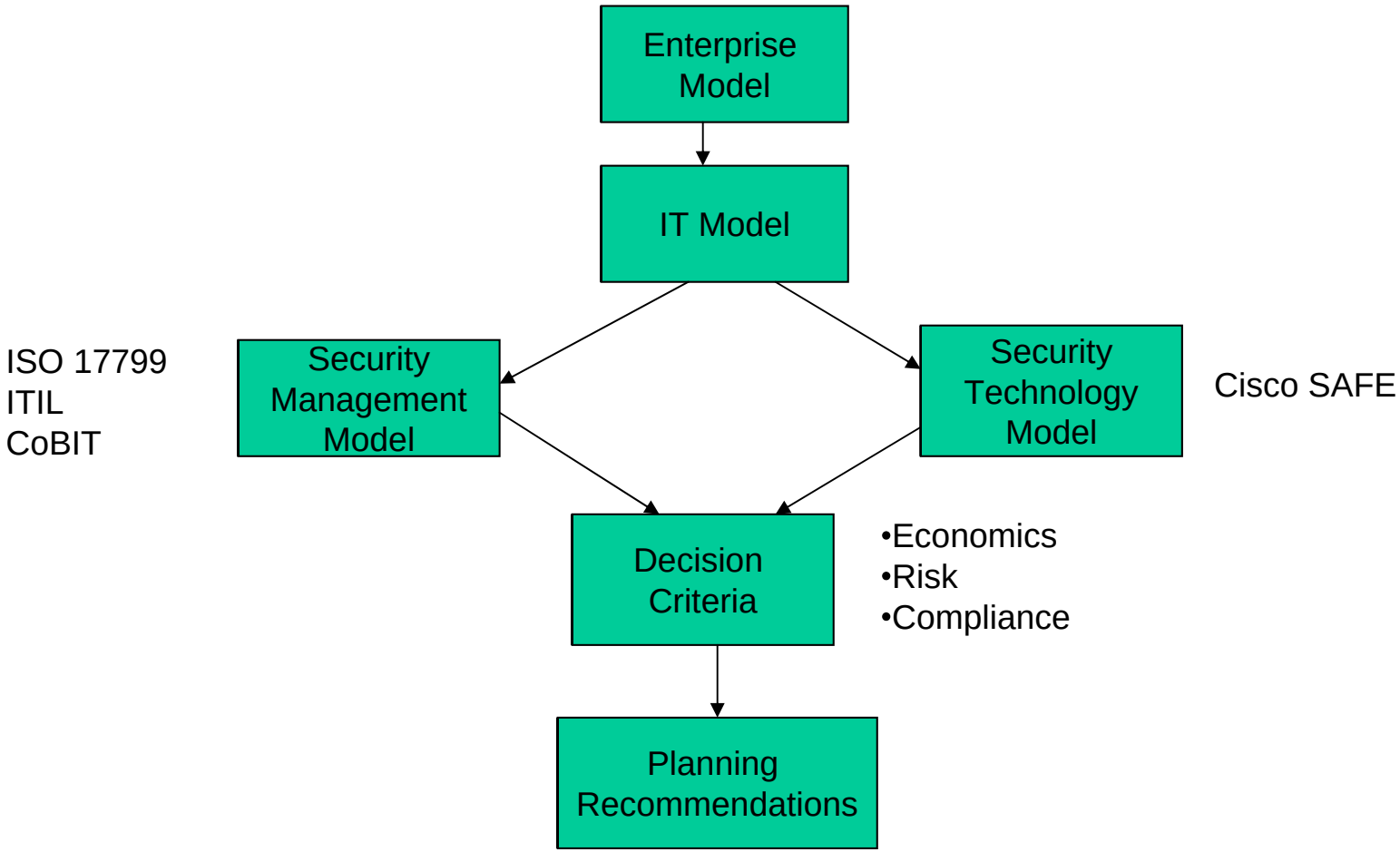
Technocratic Models

- Attempt to bring technology modeling and systems analysis methods to bear on business strategy development
- Reflect “state of the art”, hence become dated very quickly
- E.g., Information engineering adopting the data modeling techniques of structured system analysis

So much for background..

- Techniques for developing organization strategy
- Techniques for developing an IT strategy
- Where does information security fit in?
  - Tail?
  - Or Dog?

Building an IT Security Strategy



Building an IT Security Strategy

- Enterprise Model
- IT Model
- Information Security Model
  - Management
  - Technology
- Decision making criteria
- Planning recommendations (tactical plans)

Enterprise Model

- Earlier “models of business strategy” provided some
- Describe:
  - Mission, goals, objectives
  - Internal dynamics
  - External forces
- Create a coherent narrative and a guide to decision making

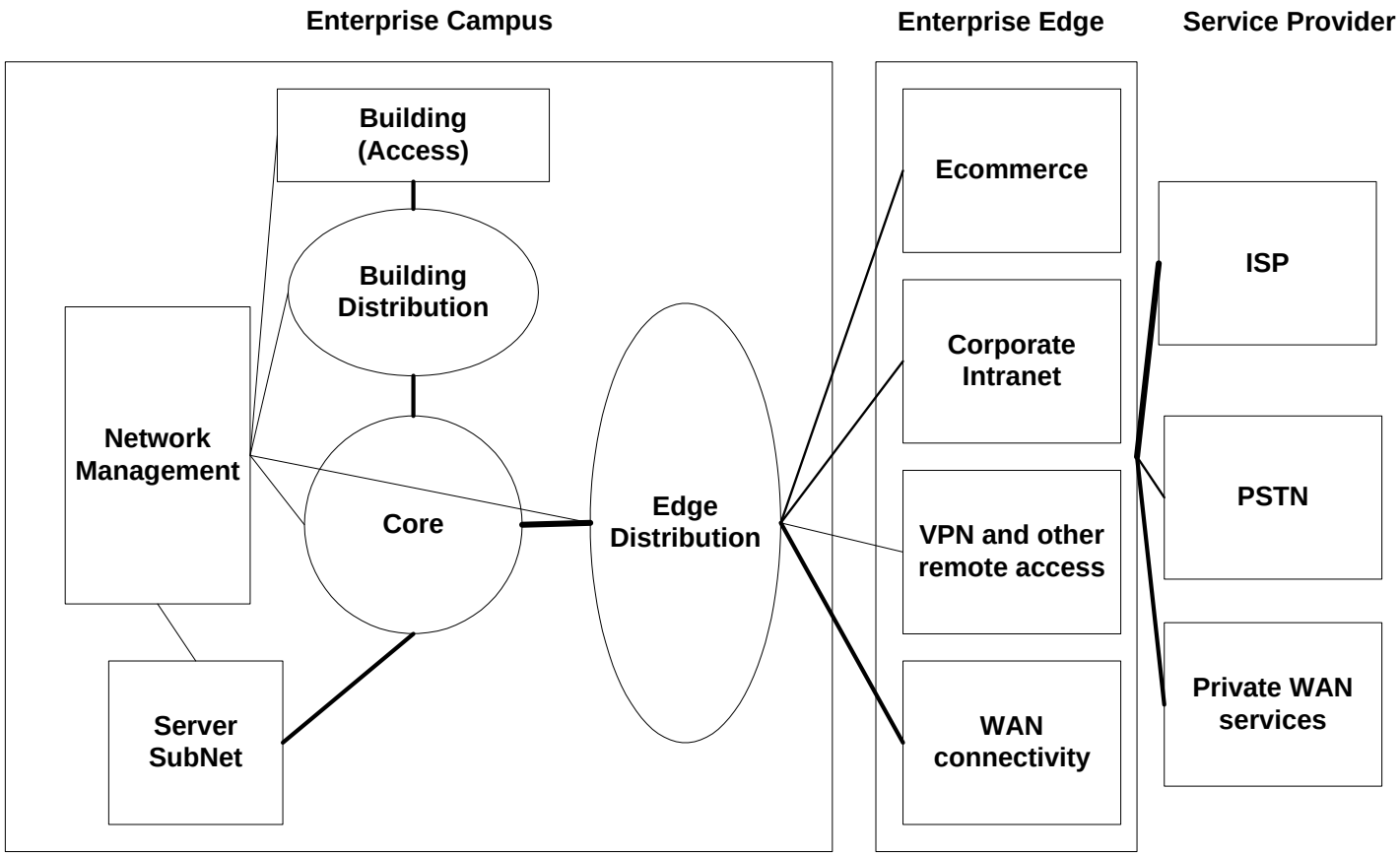
IT Model

- How does information technology support the organizational model
- How is IT managed?
- Which IT investments support the organization's strategy?

Technology Strategy

- Cisco SAFE Framework
  - Logically divide a network into functional security domains
  - Based on standard Core/Distribution/Access plus other areas for servers, DMZ, etc.
  - A way to localize security requirements and configure technical solutions

Cisco SAFE Framework



Management Strategy

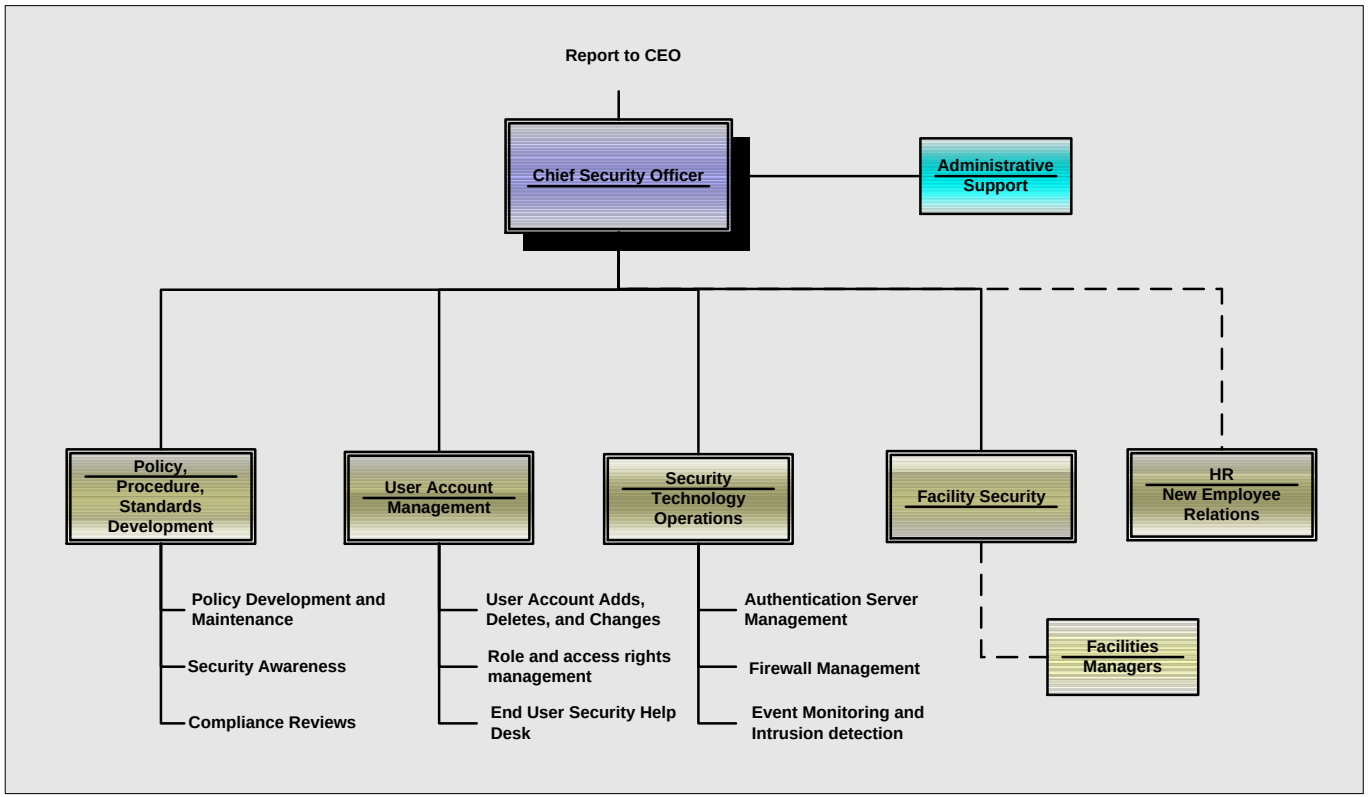
- How to manage the security program
  - Formal management structure (org chart, etc.)
  - Informal social structure
  - Scope of information security management
  - Size of security function (staffing)
  - How are decisions made?
  - How is the effectiveness of the security function evaluated

Formal Management Structure

- To whom does the senior information security executive?
- Scope of authority over IT Security
- Authority over/ relations with related functions

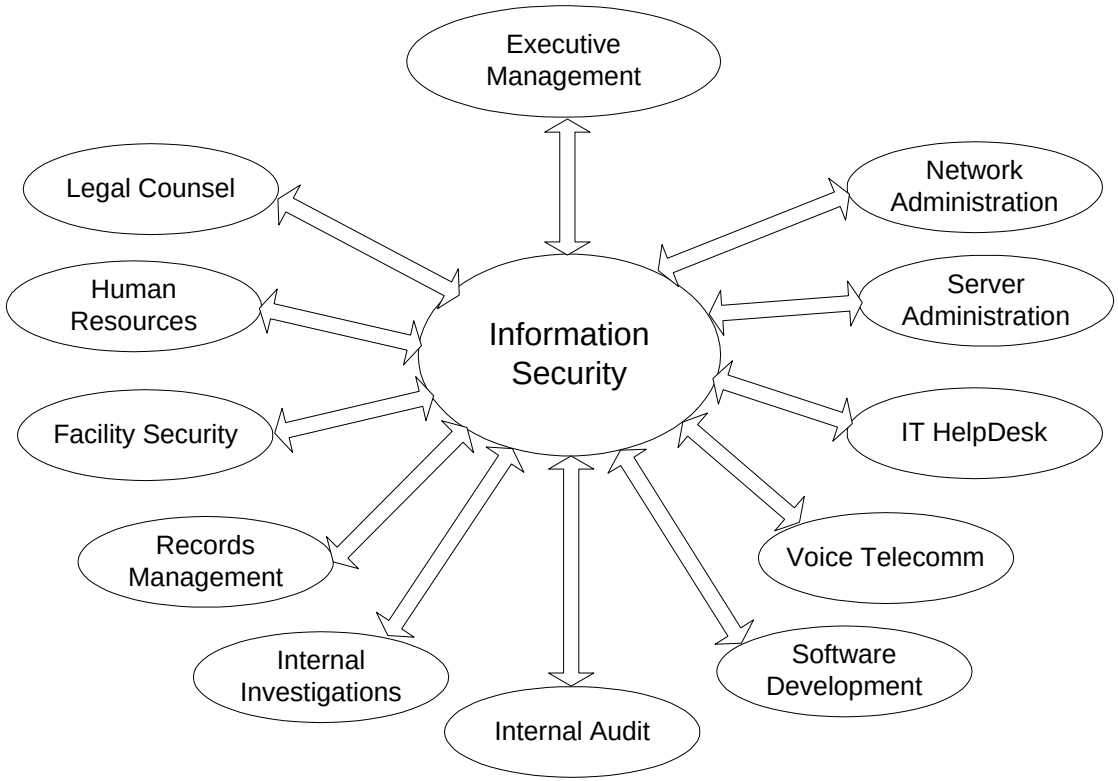
Formal Management Structure

Example IT Security Organization



Formal Management Structure

Organizational Interfaces



Informal Social Structure

- Organizational culture and values
- Always dominate over formal policies
- Organizational sociology and anthropology

Informal Social Structure

- Max Weber's forms of leadership
  - Charismatic
  - Traditional
  - Bureaucratic

Scope and Size

- For which security functions should information security be directly responsible?
- Where information security is indirectly responsible, how should this be accomplished
- Given the direct and indirect functions, how much staff is required and at what cost?

Decision making

- Combines risk analysis and economic analysis
- Security purchases a reduction in risk to information systems
- This implies two main issues:
  - How is risk managed
  - How is information assigned an economic value

Strategy and Risk

- How to measure risk
- How to determine criteria for evaluating risk vs. cost trade-offs
- How to manage cultural and psychological issues involving risk perceptions

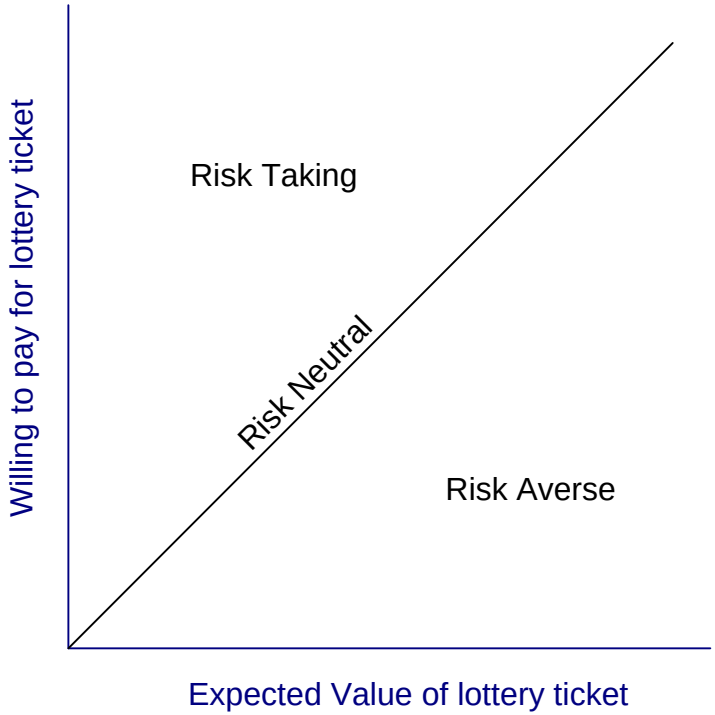
Strategy and Risk

- Classic risk formula is Annualized Loss Expectancy (ALE)
- Probability of an event times anticipated loss if event occurs over a one year period
- Implies large number of small losses are equivalent to a single, less likely large loss
- Is this valid for all (or most) cases?

Risk: Takers, Neutral, Averse

- Actual behavior vs. expected payout from a lottery
- How much is a bet on the lottery worth to you as actual cash in hand?
  - Same as expected payout = risk neutral
  - More than payout = risk taker
  - Less than payout = risk averse

Risk: Takers, Neutral, Averse



Risk

- Willingness to accept risk may depend on
  - Amount at stake
    - Risk aversion may increase as the size of the possible loss increases
  - Financial situation of individual taking risk
    - "the famous Friedman-Savage double inflection utility function"
    - Risk aversion at low and at high income levels
- Note: Risk averse managers tend to place a higher value on information
  - Ronald H. Hilton – The Determinants of Information Value: Synthesizing some General Results - 1981

Information Economics

- Can you make decisions about information based on its economic value?
- Prerequisites
  - Define information as a discrete entity
  - Assign organizational responsibility or ownership of information
  - Track the use of information within the organization

Is information an asset?

- UK Accounting Standard for Goodwill and Intangible Assets FRS10
  - Allows for valuing information as an asset
  - In one study, not a single company did so!
    - Wilson, Stenson, Oppenheim, “The Valuing of Information Assets in UK Companies”, Loughborough University, 2000
  - Requirement that information have an identifiable market value proved to be a barrier
  - Companies preferred to view information as a service than as an asset, even within IT

Why valuing information is difficult

- Information is an “experience” good
- High returns to scale
  - Hard to make
  - Easy to reproduce
- Like a public good in some ways
  - Nonrival
  - Nonexcludable

Why information security is hard – an economic view

- Paper by Ross Anderson: http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf
- Perverse incentives, “tragedy of the commons”
- Network externalities result in “winner take all” rewarding first to market and not best engineered (most secure)
- Use of “security” features to achieve other goals (vendor lockin, etc)
- Large, complex systems are more easily broken than made unbreakable

Ways to assign value to information

- Cost of production
- Market value
- Reduction in uncertainty in decision making
  - Relative to risk aversion
- Instrumental value, as the accumulated experience on how to do things “the best way”

The economics of a security breach

- Compromises of confidential information do have a negative impact on publicly traded share return!
- See:
  - The economic cost of publicly announced information security breaches: empirical evidence from the stock market, Katherine Campbell, Lawrence Gordon, Martin Loeb, and Lei Zhou, Journal of Computer Security 11 (2003) pages 431-448
  - This study covered 43 major security breaches involving 38 firms in the period January 1995 through December 2000

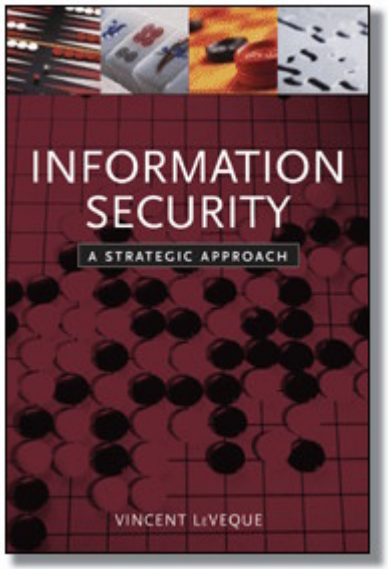
Conclusions

- Information security strategy should fit within an organization's business and IT strategies
- An information security strategy requires both a management model and a technical infrastructure model
- Decision making in information security requires understanding risk and information value, as economic and sociological concepts

Resources

- Information Security Economics http://infosecon.net/

Now a short commercial



Buy my book!

“Information Security: A Strategic Approach”
Pub: Wiley-IEEE Computer Society
ISBN: 0471736120