Risk Perception; risk assessment

Robert H. Sloan

Two loosely related topics

- FUD (Fear, uncertainty, doubt)
  - We don't know the odds, or we systematically calculate the odds wrong
  - Behavioral economics, psychology
- Risk Assessment
  - We (at least claim we sort of) know the odds of various bad things happening, now what do we do about it?

Risk Perception: The issue

- General public and experts often vary wildly on perceived risk.
  - E.g., experts would almost certainly rate driving in a car as greatest source of risk (# fatalities, lost life expectancy, whatever) among: driving in a car, radioactive waste, DNA technology, and nuclear reactor accidents
  - Survey of public would not get same result.

Human beings and fear

- We have several built-in rules of thumb
  - Representativeness heuristic
    - Assuming a "typical" instance is an extremely probable one. People will overestimate number of Chicago January days with temperatures below 20, number of criminals who are poor young men, etc.
  - Availability heuristic
  - Affect heuristic
  - Confirmation bias

and more, that affect us in general, and in our assessment of risks and of incidents in particular.

Availability heuristic

- If it's easy to think of an **example**, then it's likely, or, in other words, easily remembered = probable
  - Highjackers smashing planes into buildings
  - Anthrax attack on U.S. mail

- Earthquake insurance in major fault zones
  - What is rate of optional purchases as function of time since last big quake?
  - Why?
  - What should it be?

Affect heuristic

- Current feeling ("affect" here means feeling, in the sense of mood but shorter term) has big impact on judgment

- Good things are good: they do not pose a significant risk and they aren't terribly unlikely
- Bad things do pose a significant risk
- Winning the lottery; likelihood of terrorism
- People overestimate dangers of nuclear power, waste relative to expert opinion
- People mildly underestimate the dangers of sunbathing

Confirmation bias

- We pay more attention to data confirming opinions we already hold
  - The Red get redder; the Blue get bluer.

Public risk perception driven by

- All of above and
- Dread
  - Involuntary assumption of the risk
  - Induces feelings of dread
  - Not equitable
  - Risk not easily reduced
- Unknown
  - New risk
  - Risk unknown to science
  - Unfamiliar, not well understood

So

- Public worries a lot about
  - DNA Technology
  - Nuclear reactor accidents
  - Radioactive waste
- But not
  - Home swimming pools
  - Auto accidents
  - Power lawn mowers

Impact of *Incidents* on public

- Recency (affects availability)
- Vividness (affects availability)
- Affective saliency

- So post 9/11 U.S. citizen terrorism worries huge for 2001–2004, still bigger than expert opinion would suggest.

- All this has perhaps evolution justification, & even today "Just because you're paranoid doesn't mean they aien't out to get you."

Part 2: Risk Analysis/Assessment

Outline of Risk Analysis

- Identifying and Valuing Assets
- Identifying and Assessing Risks
  - Qualitative
  - Quantitative
    - ALE
- Managing Risk
  - Risk Avoidance
  - Risk mitigation
  - Risk Acceptance
  - Risk Transference

Identifying and valuing assets

- Some common techniques, think about how well they fit to *information assets*
  - Replacement cost valuation
  - Original cost valuation
  - Depreciated valuation: original – depreciation to date
  - Qualitative: Don't try for dollar values, rather assign priorities to assets based on their value to the organization

Identifying and Assessing Risks

- **Vulnerability** is a property (weakness) in your system
- **Vulnerability + Threat = Risk** (of security failure)
- **Assessment:**
  - **Qualitative:** analyze intangibles as well as any hard data, rate risks by priority, assign security and/or other resources accordingly
  - **Quantitative:** Typical methodology is **Annualized Loss Expectancy (ALE):**

ALE = Annualized rate of occurrence * Expected loss per incident

(ARO * SLE)

ALE: The game

- Supposed to say: Hmm. Computers and power surges. I expect it costs $100 to fix the computer ("single loss expectancy"). My wild guess: 5% chance of a meaningful power surge in a year. So ALE = 0.05*100 = $5.
- Whoops! I want to sell these guys surge protectors! Decent cheapies are $6.99–$15. I really want to sell them on these particular nice ones that are $25 each.
- I estimate the annualized rate of occurrence at 2 surges/year; ALE is $200.
  - Fork over the $25/computer!

Managing risks

- **Risk avoidance**: If, e.g., risks of employee access to email or the web while on site are too great, turn off employees' access.
- **Risk mitigation**: Preventative measures to lessen the risk. E.g., a firewall at least somewhat mitigate the risk of hackers.
- **Risk acceptance:** Where risk is judged very low probability or small loss, or very expensive. I have no earthquake insurance; university probably has no plan for meteor striking campus data records; banks expect some theft by tellers
- **Risk transference:** Most common form is insurance