

# **Security Administration**

**Jeff King**

**July 3, 2007**

# Security Plans

- Elements of Plan
  - policy – goals
  - current state – where are we?
  - requirements – recommended ways to meet goals
  - recommended controls – mapping controls to vulnerabilities
  - accountability – who is responsible for each activity?
  - timetable – when are activities done
  - continuing attention – periodically update plan
- Planners should be all stakeholders (developers, users, management)

# Business Continuity Plans

- Deal with catastrophic situations with long duration
- Identity assets and possible disruptions
- Develop strategy for mitigating disruption
  - Call center in London fails; reroute calls to Tokyo
  - Tokyo may have reduced capacity, but better than none
  - What components (technological, policy, etc) are required?
- Develop concrete plan for each situation
  - Who is in charge? What do they do?
- Recognize cost/benefit of protecting particular assets.

# Incident Response

- What is an incident? How do we know when malicious intent is involved?
- Who takes charge? What do they do?
- Other ramifications of incident? Legal? Business?
- Reflect and update security plan.

# Risk Analysis

- risk impact – loss associated with event
- risk exposure (expectation) –  $impact \times probability$
- dealing with risk
  - avoid the risk (change requirements)
  - transfer the risk to another entity
  - lower risk with controls
  - mitigate impact with response planning
- $\frac{exposure_{before} - exposure_{after}}{cost_{reduction}}$

## Risk Analysis Procedure

- Identity assets.
- Determine vulnerabilities.
- Estimate likelihood of exploitation.
- Compute expected loss.
- Survey applicable controls and their costs.
- Project savings of control.

## Why Risk Analysis?

- Improve awareness
- Relate security mission to management objectives
- Identify assets, vulnerabilities, and controls
- Improve basis for decisions
- Justify expenditures for security

## Why not risk analysis?

- Hard to get numbers right
- False sense of precision and confidence
- Immutability
- Lack of accuracy