# Information System Security Plan Steps

# STEP ONE – Understand the Asset

- Effective security begins with a solid understanding of the protected *asset* and its value
- DATA is identified as our primary asset
- Philosophically, we believe that "security should follow data"
- But we know that not all data were created equal

# STEP TWO – Identify and prioritize Threats

- Governance:
  - policy breach
  - rebellion
- Physical:
  - data theft
  - equipment theft/damage
- Endpoint:
  - theft
  - social engineering
- Infrastructure & Application:
  - theft
  - disclosure
  - DoS
  - unauthorized access
- Data:
  - unauthorized access
  - corruption/destruction

# STEP THREE – Identify and rank **V**ulnerabilities

- Governance:
  - policy loopholes
- Physical:
  - weak perimeter
  - open access
- Endpoint:
  - ignorance

- Infrastructure & Application:
  - “open” network
  - unpatched systems/OS
  - misconfiguration
- Data:
  - unencrypted storage
  - insecure transmission

# STEP FOUR – Quantify Relative Risk, ***R***

$$R = \mu VAT$$

V = vulnerability
A = asset
T = threat
$\mu$ = likelihood of T

- The greater the number of vulnerabilities the bigger the risk
- The greater the value of the asset the bigger the risk
- The greater the threat the bigger the risk

# STEP FIVE – Develop a strategy

3 virtual operational protection zones, OPZ
based on Data Classification

High
- Significantly business impact
- financial loss
- regulatory compliance

Moderate
- adversely affects business and reputation

Laptop with *High* data

Normal
- minimal adverse effect on business
- authorization required to modify or copy

Server with *Moderate* data

Types of data stored, accessed, processed or transmitted dictates OPZ

Higher Classification implies Increased Security

# STEP SIX – Establish target standards

- Seven layers of protection per zones based on COBIT, ISO 17799, FIPS 200 and NIST 800-53
  1. Management & Governance
  2. Access control
  3. Physical security
  4. Endpoint security
  5. Infrastructure security
  6. Application security
  7. Data security

Amount and stringency of security controls at each level varies with data classification

# Snippet from Data Security Standard

| Security Control | Red Zone | Yellow Zone | Green Zone |
|---|---|---|---|
| Encrypt stored data | Mandatory | Recommended | Optional |
| Limit data stored to external media | Mandatory | Recommended | Optional |
| Encrypt transmitted data | Mandatory | Mandatory | Recommended |

# STEP SEVEN – Document the plan

- Create a list of action items for the next 3 to 5 years
- Prioritize the list based on risk and reality
- Forecast investment
- Beg, kick and scream to get funding
- Implement the plan over time

Identify realistic solutions for applying the appropriate security controls at each level.