Security Process Flowchart – Steven E. Miller

Establish Organizational Context

1-A. Purpose

Confirm Organizational Mission

...to keep security planning relevant and appropriate

1-B. Scope

Review IT Role

Identify and rank importance of IT tools, data, and services used by stakeholders.

1-C. Yardsticks

Externally-based Accountability

Establish standards and reporting requirements for

- *Tech Systems*
- *Educator Tech Competency*
- *Student Tech Skills*

1-D. Service Levels

Benchmarks for IT operations

Establish levels of support required for organizational effectiveness.

Product #1:

Security Decision Guide

Benchmarks for IT operations

Risk Analysis

2-A. What's at Risk?*

Asset Inventory

- *Systems*
- *Data*
- *Physical plant*
- *Staff expertise*

2-B. What's it Worth?

Measure potential impact of threat events

...on organization if assets are...

- *Disclosed*
- *Corrupted*
- *Taken out of service.*

2-C. Assess Threats

Identify potential threat actors

- *People: accidental and intentional causes*
- *Systems: defects, weaknesses, malware (exposure to viruses, worms, etc.)*
- *Physical plant: power, floods*
- *Organization: policy, training, leadership*

Product #2:

Risk Assessment Report

Prioritized list of vulnerabilities

Risk Reduction

3-A. Security Stress Tests

Comprehensive Technical Evaluation

- *Diagnostic tests*
- *Operational Reviews*

3-B. Problem Profile

Prioritize security problems

Based on

- *Urgency*
- *Critical value*

3-C. Define Security

Establish locally-relevant standards

Based on

- *best practices*
- *local capacity and resources*

3-D. Security Triage

Required Actions: immediate or long term?

Use SecurityStandards defined above to identifyboth immediate remediations and longer-term improvements.

Product #3:

Security Action Plan

Prioritized list of actions

Crisis Management

4-A. Crisis Risk Analysis

Identify crisis risks to organizational assets.

4-B. Response Protocol

Create protocols to

- *assess & limit damage during a crisis*
- *communicate with stakeholders*

4-C. Recovery

Develop plan for post-crisis recovery

Establish levels of support required for organizational effectiveness.

4-D. Crisis Readiness

Identify requirements for:

- *Training and simulation*
- *Equipment replacement*
- *Alternate facilities*

Product #4:

Crisis Management Plan

A blueprint for organizational continuity

© 2003 Mass Networks Education Partnership

* Asset based approach draws on work done by Software Engineering Institute at Carnegie-Mellon University