A Knowledge Management Approach to IA Policy & Reporting

Briefer: Larry Johnson, J-653 (703) 767-2195
About DLA

• Defense Logistics Agency
  – 34,000 people
  – Worlds largest e-business
    • Over 5 million items in our catalog
    • 87 billion in inventory
    • 27 million transactions annually
    • 28,000 trading partners
IA Policy as a Problem Space

A major vector for IA vulnerabilities

Threats → Mitigations

Economic constraints → Technical constraints

Policy analysis

Policy formulation

Program development

Program execution
IA Policy as a Problem Space

Multiple policies can be duplicative
Policies can be obsolete
Policies can be incomplete
Policies can have inappropriate or inconsistent levels of abstraction
Policies can be misinterpreted
Knowledge Management

Policy Analysis

Policy formulation

Program development

Program execution

Construct a meta-level abstraction of the Policy chain

Independent of IA

Explicitly evaluate transformations

Extract factors that affect causality

Epistemological orientation
Case Study: DoD System Security Plans

- 600+ production (existing) LANs, systems & web sites must be certified and accredited under the DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
  - The product is a comprehensive security plan called a System Security Authorization Agreement (SSAA)
- Problems with the SSAAs:
  - Cost averages 75K per system: Effort was consuming virtually all IA resources
  - Virtually all are late
  - Huge variation in quality: two similar systems in the same enclave reported totally different
    - Threats
    - Mitigations
    - Risks
Case Study: DoD System Security Plans

- SSAAs were not designed for *existing* systems or sites
  - Phases map to new system life cycle management
    - Requirements
    - Design
    - Development
    - Testing & Implementation

- Can generate huge amount of effort with no appreciable security improvements
- Efforts were being “hand crafted”
- Each project creates their own security solution
Case Study: Solution Set

- Standardize threats, mitigations and risk analysis across DLA based upon current DoD “Defense in Depth” policy
- Map LCM phases to a process that’s relevant to existing LANs and systems
- Simplify the SSAA preparation process by an order of magnitude
  - Migrate resources from document development to implementing protection mechanisms
Case Study: Solution Set

• The **program** DLA created to accomplish these three critical success factors is called: *Metrics and Controls for Defense in Depth (McDID)*

• The **system** created to support the program is called: *Comprehensive Information Assurance Knowledge-base (CIAK)*
DLA’s IA Policy World
McDID: Using DITSCAP for Policy Integration

In the process of certifying and accrediting, all major DoD IA policies are complied with.

DITSCAP C&A
36 System Controls,
92 Site Controls

Knowledge management tool
Removes duplication, normalizes Abstraction & ensures coverage

CJCSI Metrics
Computer network Defense
IA Implementation
GIG
Defense in Depth

Best Practices
McDID
CIAK Knowledge Management Tool

Persistent linkages

DLA policy
Being created

A “meta-level” of
DoD policies

Auto-import from
Microsoft Word

DOORS object-oriented database
CIAK provides automatic configuration management & workflow.
Mapping LCM Phases to Existing LANs and Systems

1. Draft SSAA using template & tools.
2. Assess IA controls.
3. Develop implementation plans.

- **Definition**
- **Verification**
- **Validation**
- **Post Accreditation**

Traditional SSAA

- **Phase I**
- **Phase II**
- **Phase III**
- **Phase IV**

McDID

- Implement DLA standard IA controls
- Validate & Test controls
- Continuous Security improvement
CIAK decomposes documents visually
For easy navigation
CIAK

Access rights to individual objects
Can be controlled

Subordinate objects can Selectively inherit properties
Making C&A Easier
(but more comprehensive & consistent)

1. Write the enterprise parts
   - Threats
   - CONOPS
   - Mitigations
   - Risk Assessment

2. Translate narrative
   Into “fill in the blank”

3. Provide templates
   (for both authors & evaluators)

4. Use a web-based
   Automated configuration
   Management system for
   workflow

“Standard” SSAA Outline
Policy Simplification

Turn technical documentation into “fill in the blank”

**Template SSAA Security Plan**

17 spreadsheet templates

In one Excel workbook
Policy Simplification

SSAA’s can go directly in CIAK via the web for automated configuration management and workflow
Policy Simplification

Self assessment & plan of action tool
3D IA Architecture
CIAK Architecture

Data management

Object data
- DOORS (QSS Inc.)
- Bridge
- Clearcase (Rational)
- Relational data
- SQL Server (Microsoft)
- Data visualization
- Netviz 3D (Netviz)

Internet Publishing

- DOORSNet
- Microsoft IIS
- Netviz Publisher
Status

• CIAK recently came on-line in early December
• First production system showed 90% savings in time and cost
• CIO briefed and requested Deputy Director briefing
• Planning integration with DLA’s Asset Management Program
Other Uses?

• Taxonomic based research
  – Threat taxonomies
  – Attack signatures

• A possible mechanism for protection against litigation
  – Reasonable
  – Prudent

• Mapping complex policies
  – Common Criteria to BSI 7799

• Integration with other automated tools
  – Asset management
  – Configuration management
Conclusion

• Policy is a major vector of IA vulnerabilities in large, complex organizations
  – A formal policy analysis methodology based upon knowledge management tools (particularly object oriented databases) can substantially reduce policy based vulnerabilities
  – Tools are very inexpensive & easy to use
• DLA’s McDID/CIAK programs is showing some early successes
  • Large delta in time & cost
  • Standardized security across sites & systems
  • Web-based workflow & configuration management
• DLA would like to see the IA community adopt formal policy analysis methodologies
Points of Contact

- **Larry Johnson**
  - (703) 767-2195
  - Larry_johnson@hq.dla.mil
- **Glenda Turner (Booz Allen & Hamilton)**
  - (703) 289-5279
  - Turner_glenda@bah.com