Beyond Good Practice:

Why HIPAA only addresses part of the data security problem

Jeff Collmann, Ph.D.

ISIS Center,

Georgetown University Medical Center

Beyond Good Practice

- HIPAA: the difficulties of good practice
- Software vulnerabilities in biomedical devices
- Organizing network operations and security

Health Insurance Portability and Accountability Act of 1996

- Prevent loss of health insurance upon change in jobs
- Administrative Simplification Regulations
  - Transaction and Code Set Standards
  - Privacy of all individual health information
  - Security of electronic individual health information
  - Identifiers

HIPAA Security as Good Practice

- No data security standards in 1996
- HHS sought industry advice, including NIST, DoD, textbooks, commercial practice, emerging guidelines
- Health care industry behind commercial practice
- Final Security Rule: February 2003
- Compliance date: April 21, 2005

HIPAA Security as Good Practice

- Developing administrative judgment: What but not how
  - 22 Standards
  - 40 Implementation specifications
  - Required and Addressable
- Three types of rules
  - Administrative
  - Physical
  - Technical

HIPAA Security as Good Practice

- Standard: Security Management Process

  Text: “Implement policies and procedures to prevent, detect, contain, and correct security violations.”

- Implementation Specifications: Required
  - Risk Analysis
  - Risk Management
  - Sanction Policy
  - Information System Activity Review

HIPAA Security as Good Practice

- Standard: Transmission Security

  Text: “Implement technical security mechanisms to guard against unauthorized access to protected health information that is being transmitted over an electronic communications network.”

- Implementation Specifications: Addressable
  - Integrity Controls
  - Encryption

HIPAA Security as Good Practice

- HIPAA's heart: managing data security risks
  - Adapt to scale of operations
  - Assess and learn to manage new threats and vulnerabilities to breaches of confidentiality, integrity and availability using good practice

Difficulties of Good Practice

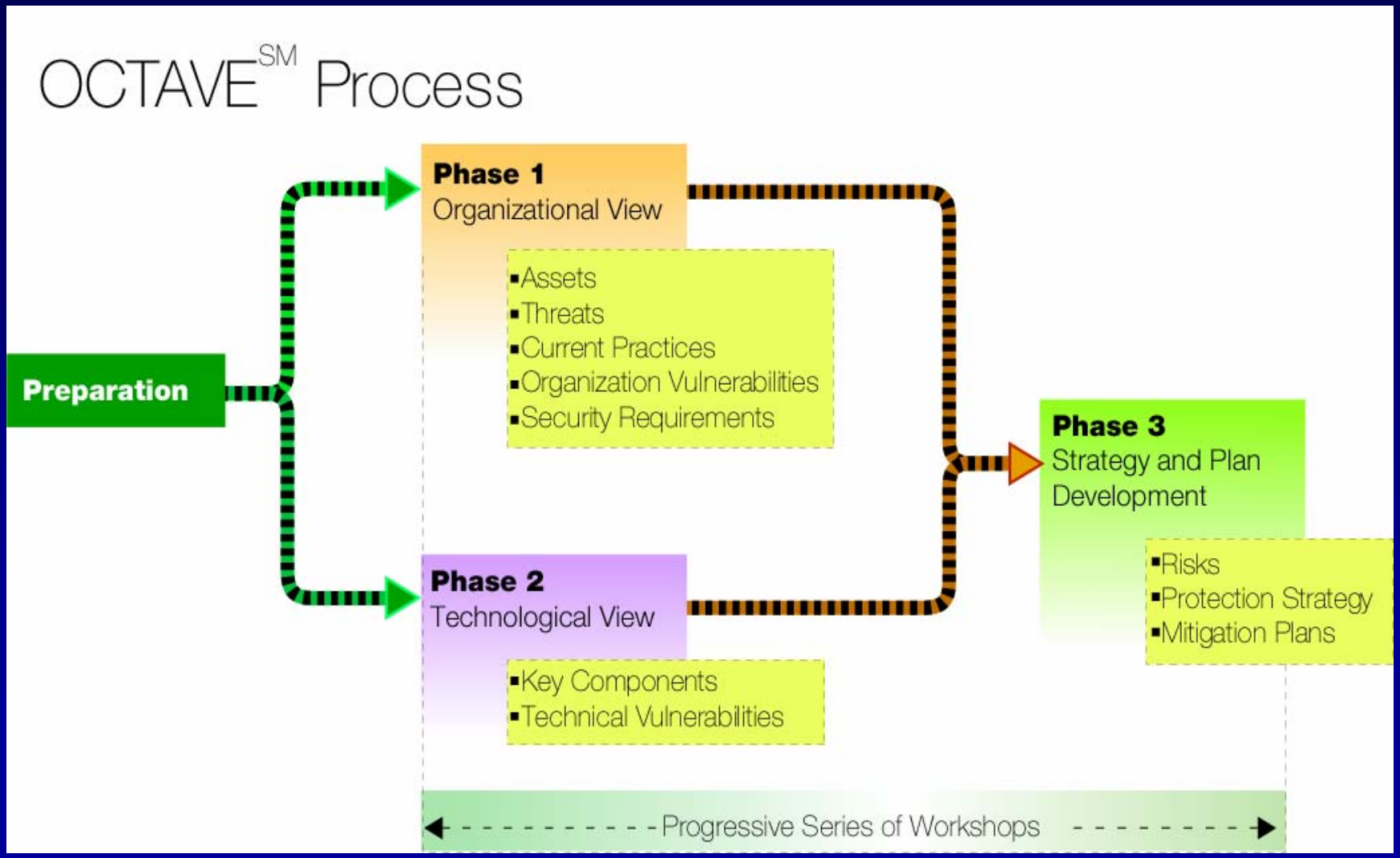
- Risk Management
  - Ongoing cycle of assessing, implementing, monitoring, and revising
  - Assesses technical and organizational threats
    - IT specialists conduct technical vulnerability scans
    - Multidisciplinary team should conduct comprehensive risk assessments
  - Requires new types of work among new constellations of people

Difficulties of Good Practice

- OCTAVE[sm]: self-directed information security risk assessment process
  - Comprehensive approach
  - Multidisciplinary team

SM - Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

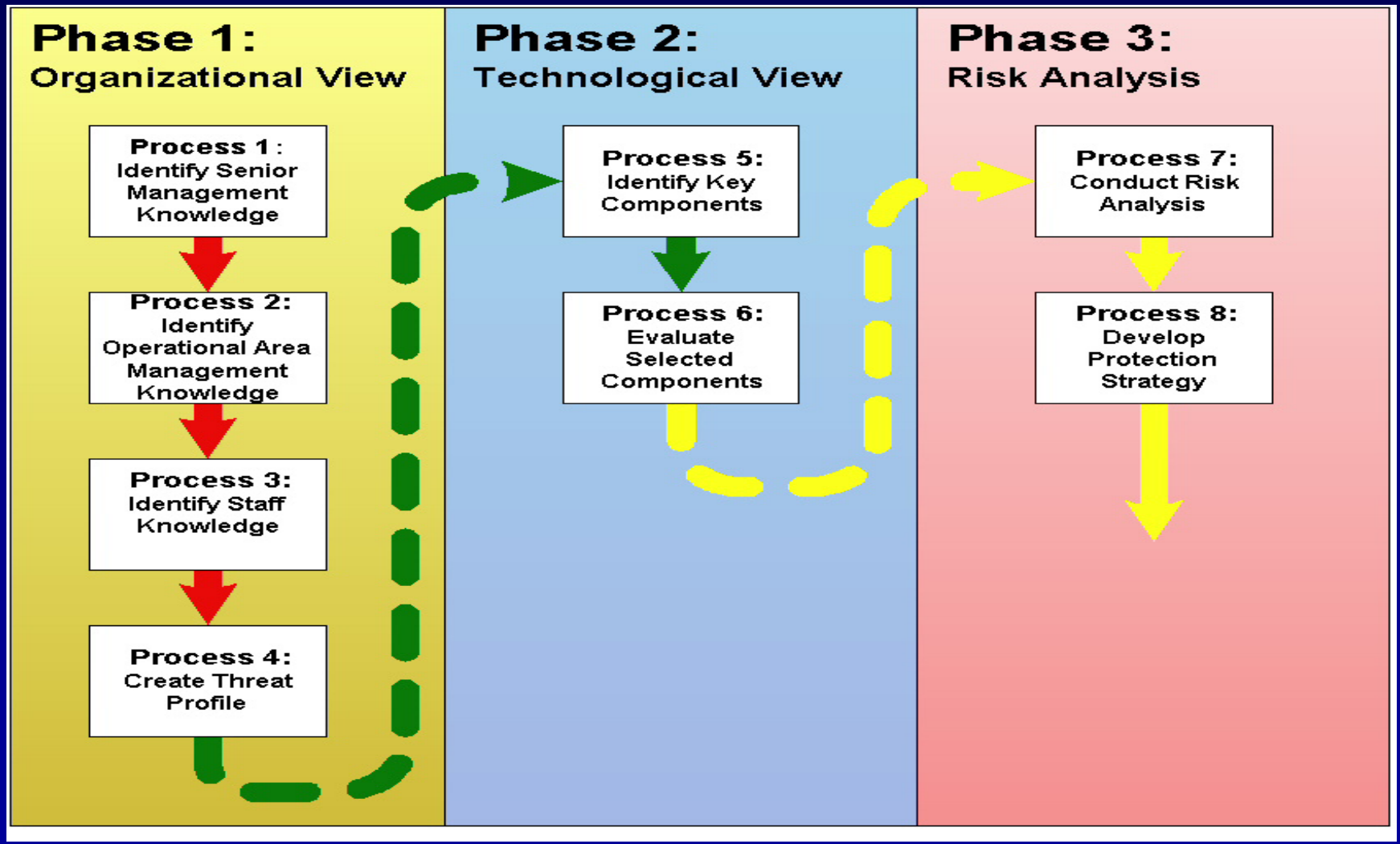
Difficulties of Good Practice



Difficulties of Good Practice

- An interdisciplinary team
  - Clinical staff
  - Health information managers
  - Information technology staff

Difficulties of Good Practice



Difficulties of Good Practice

- OCTAVE[sm]
  - Integrates mission with information assets, business process and security risk management
  - Builds consensus from diverse perspectives on information management
  - But, entails costs
    - Much time and effort across the enterprise
    - Productivity losses of staff from primary duties
    - Staff resistance
  - Fails if relegated to IT only

Beyond Good Practice

- Software vulnerabilities in Computerized Biomedical Devices
- Approaches to organizing network operations and security

Vulnerabilities in Biomedical Devices

- Medical devices subject to FDA regulation
  - 510K review for safety and efficacy
  - Software “patches” require testing and revalidation
  - Only vendors can perform repairs, testing and revalidation
  - Physicians worry about patient safety
  - Medical devices with unpatched software pose threat to entire network

Vulnerabilities in Biomedical Devices

- Medical devices subject to FDA regulation
  - Vendors not include this type of repair and testing in standard maintenance agreement
  - Negotiations among vendors and customer representatives (VHA, DoD, HIMSS) just begun
  - Vulnerabilities proliferating

Vulnerabilities in Biomedical Devices

- Does this pose a major problem for networked systems?
- Air Force TCNO alerts that affected medical devices: 15 April 2002 to 14 April 2003

Type of Operating System	Average Alerts per month
UNIX	.83
Windows	3.08
Total	3.91

Vulnerabilities in Biomedical Devices

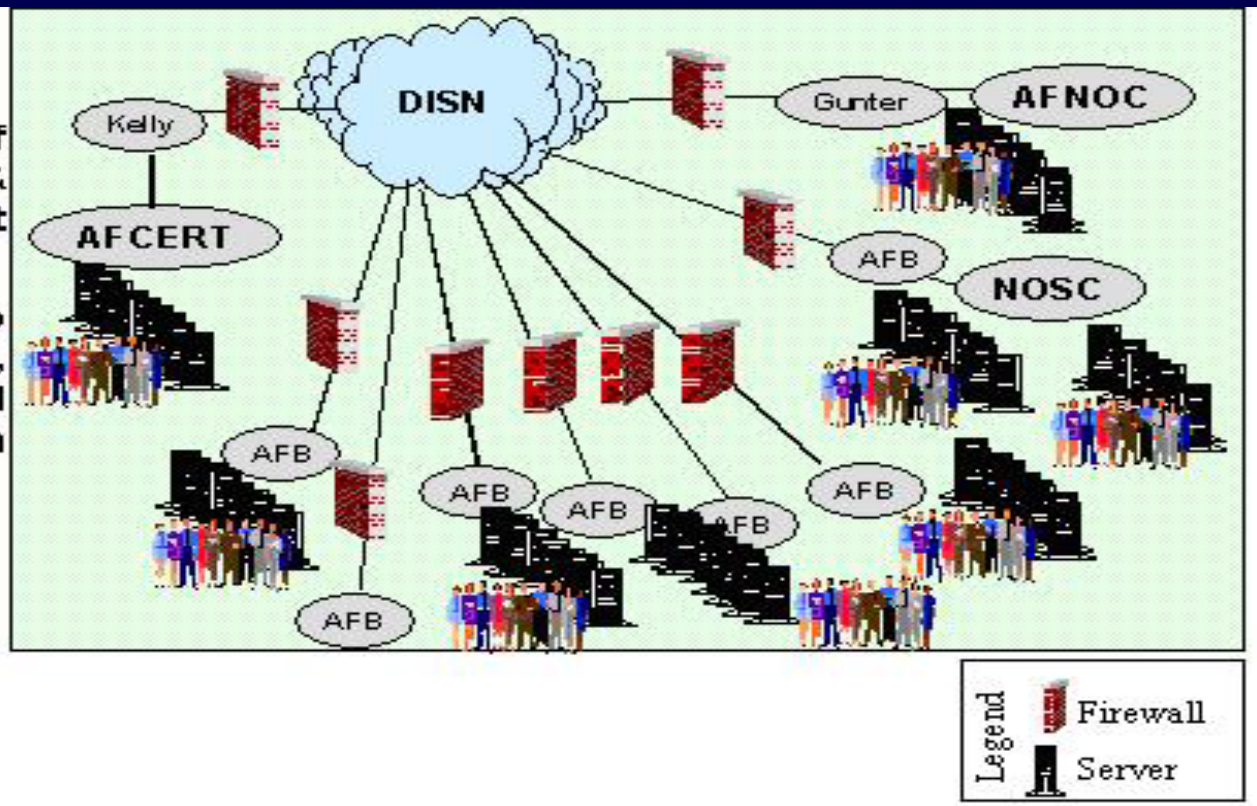
- "Revolving Threat" for Air Force Medical Service
  - Waiver can extend time for individual device
  - Before existing patches installed and tested, new vulnerabilities emerge
  - Number and time required for patches creates chronic problem for large networks with tens or hundreds of medical devices
  - Thus, performing the good practice of applying patches cannot alone secure such medical networks
- Requires contractual and architectural solutions

Architecting Reform

- “Good practice” does not address the architecture of network operation and security management
- “ One Air Force, One Network” program redirects network management from decentralized to centralized approach

Architecting Reform

- Lots of people & equipment
- Hard to defend, operate and maintain

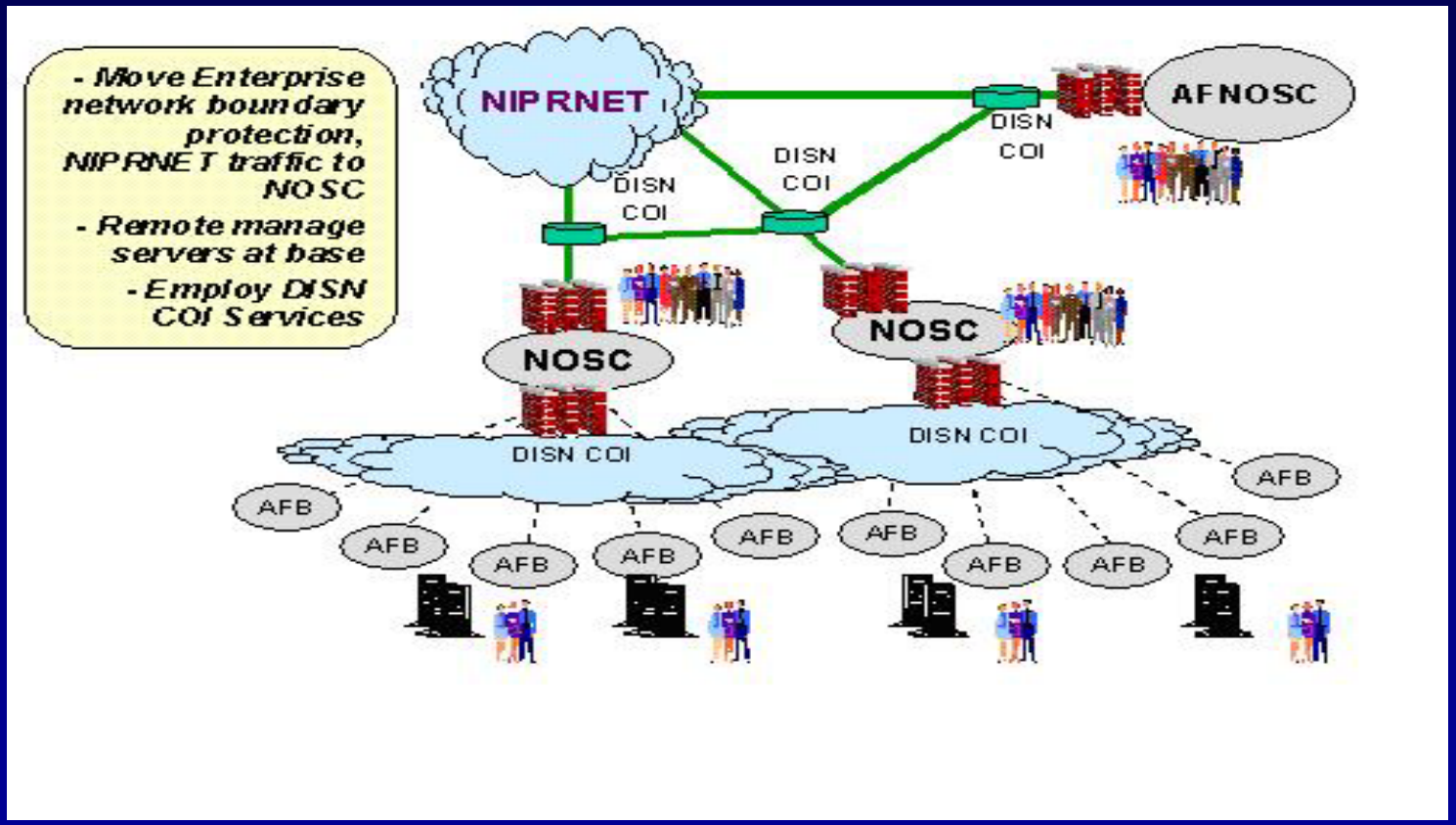


Existing decentralized network management architecture

Architecting Reform

- Each Air Force facility develops its own approach to network management and security, including military treatment facilities
- Great complexity, cost, and autonomy
  - Great diversity in hardware, software and local architecture
  - No central visibility of expense or bulk discounts
  - Little central oversight of activities or effectiveness
- Maximum flexibility to respond to local conditions

Architecting Reform



"One Air Force, One Network" centralized three-tiered management

Architecting Reform

- Air Force Communications Agency develops common approach to network management and security, including military treatment facilities
- Less complexity, cost, and autonomy
  - Common approach to hardware and software producing unified deployment and bulk discounts
  - Centralized budgeting
  - Centralized management based at headquarters of 13 Air Force Major Commands
- Minimum flexibility: Functional adaptations require negotiation with central command (eg HIPAA or biomedical devices)

Conclusions

- Implementing good information security practice in health care organizations requires new types of work among new constellations of people
- Networked, computerized medical devices pose chronic security vulnerabilities to their host networks
- Managing network operations and security requires balancing flexibility with central control