The Art of Information Security: A Strategy Brief

资艺安讯术全

Uday Ali Pabrai, CISSP, CHSS

ecfirst.com HEALTHCARE

Healthcare Security Challenges

- Password management
- InfoSec policies
- Contingency plans
- Malicious software
- Wireless proliferation
- Audit capabilities
- IT staff's security capabilities

ecfirst.com
HEALTHCARE

Security Today

- “99% of all reported intrusions result through exploitation of known vulnerabilities or configuration errors, for which safeguards and countermeasures are available”

NIST

- “The health care industry was subject to the third highest number of severe events”

Symantec

ecfirst.com
HEALTHCARE

Standards & Regulatory Compliance

Seriously influence security architecture priorities:

- ISO 17799/BS7799
- HIPAA
- FISMA
- Sarbanes-Oxley
- GLB
- California Privacy Laws

ecfirst.com
HEALTHCARE

ISO 17799 and BS 7799 Security Standards

Covers Ten Areas:

1. Security Policy
2. Security Organization
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Computer & Network Management
7. System Access Control
8. System Development and Maintenance
9. Business Continuity Planning
10. Compliance

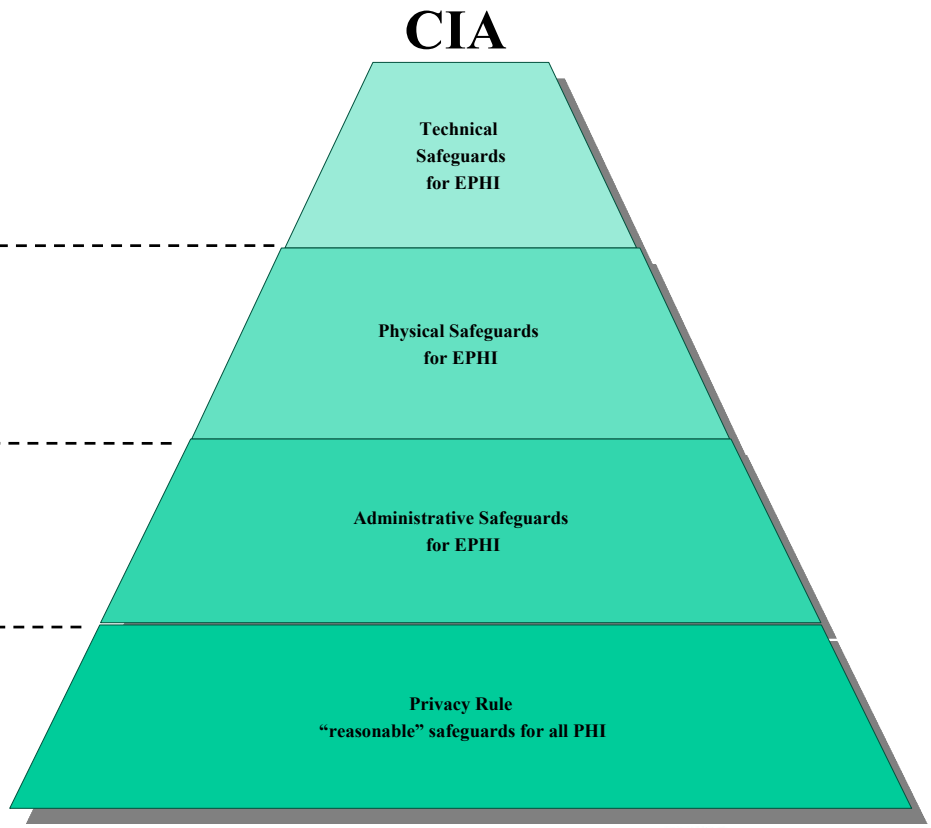
ecfirst.com
HEALTHCARE

HIPAA Security

- Access Control
- Audit Control
- Integrity
- Person or Entity Authentication
- Transmission Security

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device & Media Controls

- Security Mgmt. Process, Sec. Officer
- Workforce Security, Info. Access Mgmt.
- Security Training, Security Incident Proc.
- Contingency Plan, Evaluation, BACs



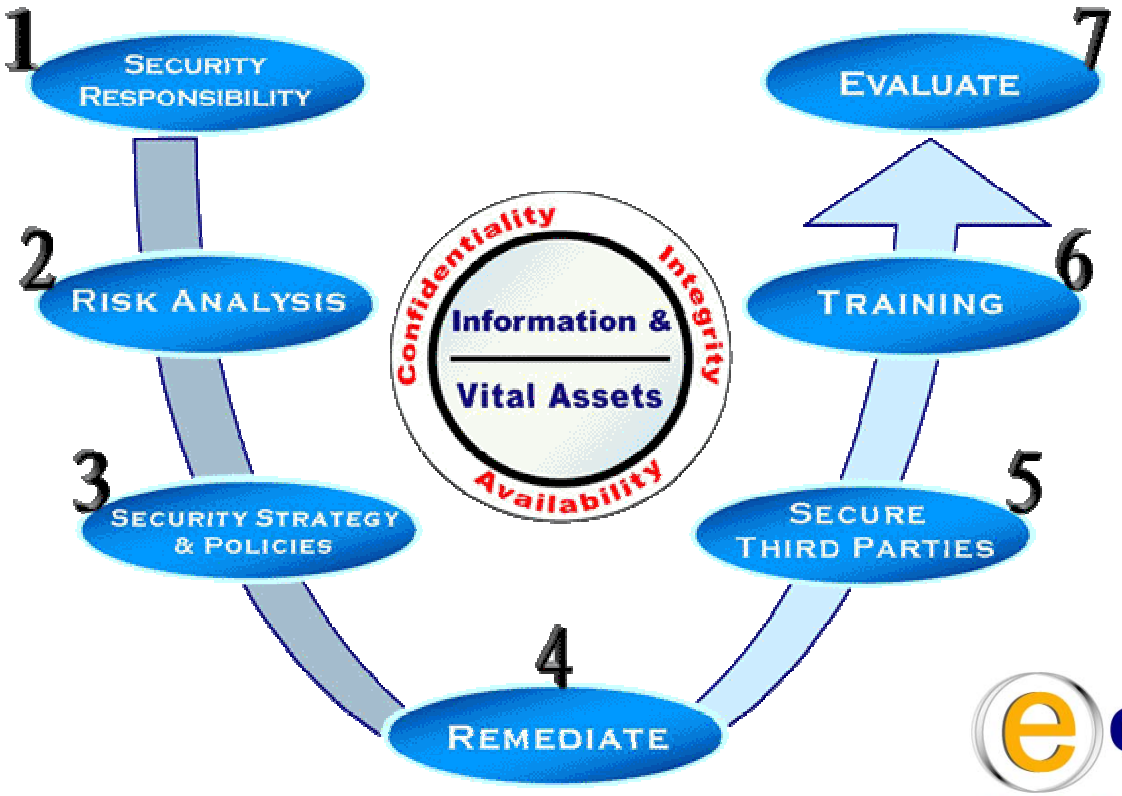
ecfirst.com
HEALTHCARE

FISMA

- The Federal Information Security Management Act (FISMA) is Title III of the U.S. E-Government Act (Public Law 107-347)
- It was signed into law by U.S. President George W. Bush in December 2002.
- FISMA impacts all U.S. federal information systems
- The FISMA legislation is about protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide CIA

Enterprise Security Roadmap

The Seven Steps to Enterprise Security™



ecfirst.com
HEALTHCARE

Risk Analysis

- "Every covered entity must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of its electronic Protected Health Information (EPHI)"

  HIPAA Security Rule

- **Not just a paper exercise**
- **Technical Review must be completed**

ecfirst.com
HEALTHCARE

Security Strategy and Policies

Activities	CIA	Target Audience
Document security procedures Develop plans for physical security	Procedures	Security practitioners
Determine gaps that need policies Validate contingency and other plans Align policies with strategy	Security Policies	Department heads
Align strategy with business goals Analyze technology architecture Evaluate role of third parties	Security Strategies	Security Officer
Understand the business Understand future goals	Business Vision	Executive management

ecfirst.com
HEALTHCARE

Contingency Plan

- It is a Federal law that must be complied with
- A HIPAA Security Rule Standard that includes:
  - Data Backup Plan (R)
  - Disaster Recovery Plan (R)
  - Emergency Mode Operation Plan (R)
  - Testing and Revision (A)
  - Applications and Data Criticality Analysis (A)
- Requirements also further identified under Physical and Technical Safeguards

Core Objectives

- Must establish policies/procedures for responding to an emergency that damages systems that contain EPHI
- Core objectives include the capability to:
  - Restore operations at an alternate site
  - Recover operations using alternate equipment
  - Perform some or all of the affected business processes and associated EPHI using other means
- Must develop a coordinated strategy that involves plans, procedures and technical measures to enable the recovery of systems, operations, and data after a disruption

Typical Security Remediation Initiatives

- **Launch Activities**
  - Deploy Firewall Solutions, IDS/IPS
  - Secure Facilities & Server Systems
  - Deploy Device & Media Control Solutions
  - Implement Identity Management Systems
  - Deploy Access Control Solutions
  - Implement Auto-logoff Capabilities
  - Deploy Integrity Controls and Encryption
  - Activate Auditing Capabilities
  - Test Contingency Plans

ecfirst.com
HEALTHCARE

Wireless Challenges

- **Lack of user authentication**
- **Weak encryption**
- **Poor network management**
- **Vulnerable to attacks:**
  - Man-in-the-middle
  - Rogue access points
  - Session hijacking
  - DoS

Wireless Strategy

- **Conduct risk analysis**
- **Develop security policies**
  - Wireless
    - Mobile devices
  - Encryption
- **Remediation: Design infrastructure**
  - Firewall
  - IDS
  - Wired network

Secure Third Parties

- **Review existing Business Associate Contracts (BACs) or equivalent**
  - Privacy compliance should have covered most of these relationships
  - Verify the flow of your sensitive information to BAs
- **BAs are part of a Chain of Custody**
  - Don't be the "weakest link"
  - Be sure to pass along requirements to protect sensitive to your subcontractors

ecfirst.com
HEALTHCARE

Train Workforce

- **Establish Processes for:**
  - Security Reminders
  - Protection from Malicious Software
  - Login Monitoring
  - Password Management

Evaluate & Audit

- **Establish Processes for:**
  - Risk Management
  - Audit

- **Deliverables:**
  - Ensure compliance with legislation(s) and standard(s) as required
  - “Close and Lock” all Security Gaps

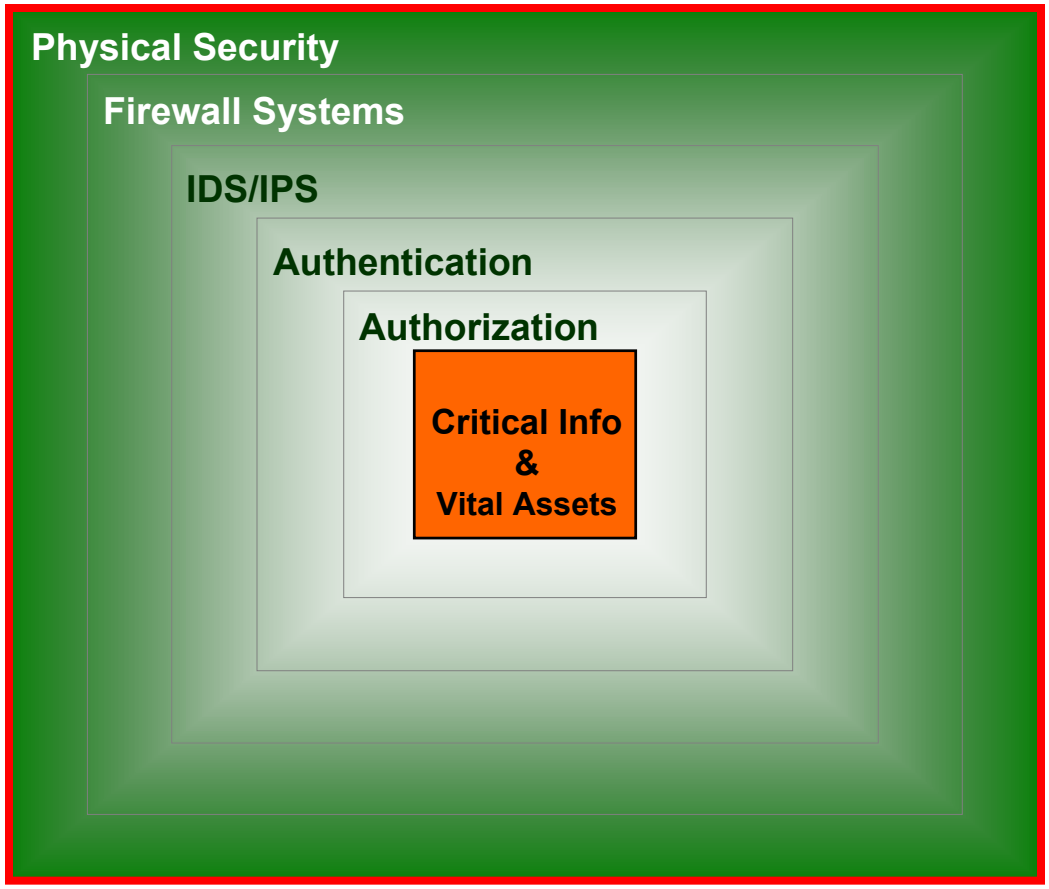
ecfirst.com
HEALTHCARE

The Importance of Audits

- Audit provide insight into vulnerabilities of an organization
- Audit on a regular basis
- Audits conducted must be thorough and comprehensive
- Strong audit trails help the entity ensure the CIA of sensitive information and other vital assets
- Key to responding to Security incident/complaint

ecfirst.com
HEALTHCARE

Defense In-Depth



ecfirst.com
HEALTHCARE

Summary: Serious Risk

- Centralize management of ALL critical servers, Internet access, wireless APs
- Ensure secure flow and storage of not just EPHI, but all vital information
- Recognize IT as a fast emerging:
  - Strategic asset, Critical asset
- Raise employee communication & training, morale
- **Security: An Executive Priority**

ecfirst.com
HEALTHCARE

Enterprise Security Goals

Establish your enterprise security objectives.

These may include:

1. Ensure confidentiality, integrity & availability of all sensitive business information
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of information
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required
4. Ensure compliance with legislations and standards as required

CIA - Security

ecfirst.com
HEALTHCARE

Thank You!

The Art of Information Security

Available ONLY at www.ecfirst.com

Pabrai@ecfirst.com

ecfirst.com
HEALTHCARE