Regulatory Compliance & Information Security

Uday Ali Pabrai, CISSP, CHSS

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

NIST

Increased dependence on electronic information and infrastructure
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
Standards & Regulatory Compliance

Seriously influence security architecture priorities:

- ISO 17799/BS7799
- HIPAA
- FISMA
- Sarbanes-Oxley
- GLB
- California Privacy Laws
ISO 17799 and BS 7799 Security Standards

• Is an international security standard that was published in December 2000

• Provides an exceptional framework for an organization to base their security infrastructure
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
10. Compliance
HIPAA

• HIPAA law has specific requirements for the protection of medical records

• HIPAA includes requirements for:
  – Transactions & Code Sets
  – Identifiers
  – Privacy
  – Security

• HIPAA Privacy Rule enforced effective April 13, 2003

• HIPAA Security Rule enforced effective April 21, 2005
HIPAA Security

• HIPAA Security Rule focus:
  – Only EPHI
  – Confidentiality, Integrity AND Availability (CIA)

• Summary: *CIA of EPHI*
  – In transit or storage
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
- Contingency Plan, Evaluation, BACs

CIA

- Technical Safeguards for EPHI
- Physical Safeguards for EPHI
- Administrative Safeguards for EPHI
- Privacy Rule
  “reasonable” safeguards for all PHI
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.
FISMA requires each U.S. federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems. These systems include those that support the operations and assets of the agency. U.S. federal agencies must be compliant with FISMA requirements. FISMA is all about information security.
SOX & Security

- Sarbanes-Oxley Act of 2002 is having an impact on an organization’s IT, especially security systems, practices and controls.
- Section 404 is a critical part of legislation
  - Requires an internal control report
- Areas of security that require particular attention include:
  - Secure identity management
  - Data integrity
  - Automated audit capabilities
Enterprise Security Roadmap

The Seven Steps to Enterprise Security™

1. Security Responsibility
2. Risk Analysis
4. Remediate
5. Secure Third Parties
6. Training
7. Evaluate

Confidentiality, Integrity, Availability
Information & Vital Assets
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
Security Strategy and Policies

**Activities**

- Document security procedures
- Develop plans for physical security
- Determine gaps that need policies
- Validate contingency and other plans
- Align policies with strategy
- Align strategy with business goals
- Analyze technology architecture
- Evaluate role of third parties
- Understand the business
- Understand future goals

**CIA**

**Target Audience**

- Security practitioners
- Department heads
- Security Officer
- Executive management

---

*ecfirst.com*
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

- **Enterprise Security Priorities**
  - 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
Authentication factors may be one or more of the following:

- Something you know (knowledge)
- Something you have (possession)
- Something you are (person)

Strong authentication solutions include:

- Tokens
- Smart cards
- Biometrics
Tokens

• Dual-factor or two-factor authenticators
• To use you need the token and you need to know something (i.e. PIN)
• Token generates unpredictable, time-sensitive number every 60 seconds
• User enters userID and their passcode
  – Passcode consists of PIN followed by code in token
Smart Cards/Badges

- Smart cards can today be integrated with:
  - Photo IDs
  - Magnetic strip
  - Company logo
  - Proximity cards

- Terrific “container” for credentials
- Addresses both network and physical security
- Billions in use today
Biometrics

- It is about verifying the identity of an individual based on measurable physiological and/or behavioral characteristics.
- A security mechanism that supports the authentication security service.
Federated Identity Management

• Overcomes the challenges of collaborative business environment
• Enables organizations to share trusted identities across enterprises
  – Outsourced providers
  – Supply chain partners
  – Autonomous business units
Identity Management
Best Practices

- Use multi-factor authentication
- Track method from issuance to deactivation
- Manage emergency access procedures
- Ensure logging
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
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
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
Defense In-Depth

Physical Security
Firewall Systems
IDS/IP
Authentication
Authorization
Critical Info & Vital Assets
Thank You!

Contact Information:
Lorna.Waggoner@ecfirst.com