Questions HHS May Ask in a HIPAA Audit: Critical Steps for Compliance

ecfirst.com

Uday Ali Pabrai, CISSP, CSCS
Author, The Art of Information Security

Do These Capabilities Exist?

- Risk assessments and analyses completed? Frequency?
- Employee violations (sanctions policy)
- Recording and examining activity in information systems
- Preventing, detecting, containing and correcting security violations
- Creating, documenting and reviewing exception reports or logs
- Inactive computer sessions (periods of inactivity)
- Monitoring systems and the network
- Physical safeguards for access to data center
- Establishing and terminating users' access to systems housing EPHI
- Emergency access to electronic information systems
- Establishing security access controls
- Remote access control
- Wireless security

Documentation...

- List of systems that house EPHI data
- List of terminated employees
- List of all new hires
- List of encryption mechanisms use for EPHI
- List of authentication methods used to identify users authorized to access EPHI
- List of outsourced individuals and contractors with access to EPHI data, if applicable
  - Include a copy of the contract for these individuals
- List of transmission methods used to transmit EPHI
- IT organizational chart
- Entity wide security program plans (e.g System Security Plan)
- List of all users with access to EPHI data. Please identify each user's access rights and privileges
- List of systems administrators, backup operators and users
- List of antivirus servers, including their versions
- List of software used to manage and control access to the Internet
- List of users with remote access capabilities
- List of database security requirements and settings
- List of all servers
- **Patch management capabilities**

Under Siege, Rising Threat

- Large, multipurpose attacks on network perimeters
- Rising threat includes focused attacks on client-side targets
- Targeted attacks on Web applications and Web browsers are the focal point for cybercriminals
- Threats are both “insider” and “outsider”
- Healthcare industry is rich in “identity” information

How confident are you about your organization’s information security posture?

Wireless Challenges

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

HIPAA's Contingency Plan Standard

- Struggle to complete comprehensive Business Impact Analysis (BIA)
- Lack of updated contingency plans
- Typically fail to identify the IT Business Continuity (e.g. CBCP)

Where is the alternate data center?

Technology Challenges

- **Too many servers**
- **Too many applications**
- **Too many PCs to maintain and manage**
- **Mobility of devices is rapidly increasing**
- **Storage demands are increasing fast**
- **Highly specialized technical skills required**
- **Serious lack of redundancy**

SOX to PCI: May Impact Your Organization…

- 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
- The Payment Card Industry (PCI) Data Security Standard (DSS) enables merchants and service providers to assess their security status by using a single set of security requirements for all payment organizations
- 12 information security requirements have been defined
- The requirements apply to all members, merchants, and service providers that store, process, or transmit cardholder data

U.S. Government Requirements

- 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

State Legislations May be the Driver?

- 39 States now have privacy and security regulation
- State regulations typically requires organizations conducting business in the State to disclose any security breach that occurs to any resident of this State whose unencrypted personal information was, or is, reasonably believed to have been acquired by an unauthorized person
- Regulations may further require that organizations take “reasonable precautions” to protect residents’ personal data from modification, deletion, disclosure, and misuse rather than just report on its disclosure

The Global Information Security Standard

ISO 27002 Covers These Areas:

1. Security Policy
2. Organizing Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

Information Security Posture?

- State of information security today:
  - Information security executives have more information than ever – but that does not mean they know what to do with it
  - The bigger the organization the more it watches its employees
    - Dramatic rise in surveillance (tracking workers information access)
  - Security executives still have difficulty:
    - Identifying who is attacking them
    - Where the attack is coming from
    - How the attack is being executed
  - Firewalls/log files/IDS are typically the way attacks are discovered
- **Compliance establishes minimal capabilities to deter and detect attacks**

Recommendations

Technology Architecture

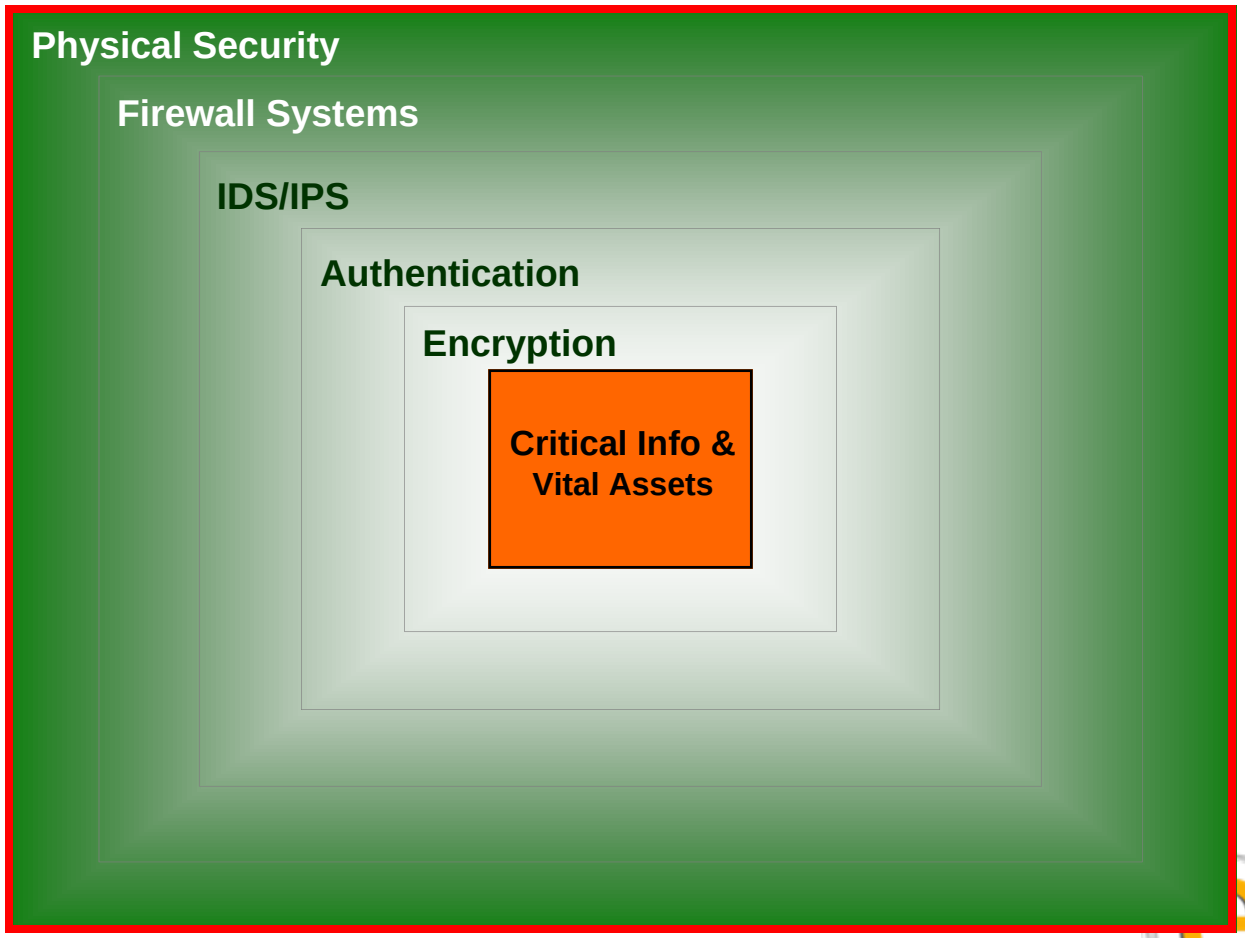
- "Thin is In"
- Bring the complexity to the data center
- Reduce the number of servers
  - Virtualization
  - Blade servers
- Plan for multi-tier storage architecture
- In new acquisitions, bake in:
  - Security
  - Compliance
  - Redundancy
- Focus on security appliances, simplify maintenance and support

Typical Security Remediation Initiatives

Typical Priorities

- Deploy Firewall Solutions, IDS/IPS
- Secure Facilities & Server Systems
- Deploy Device & Media Control Solutions
- Implement Identity Management Systems
- Deploy Single Sign-On (SSO) and Context Management Solutions
- Implement Anti-spam, Anti-virus, Content Management Capabilities
- Deploy Integrity Controls and Encryption
- Activate Auditing Capabilities
  - Both system as well as record access
- Test Contingency Plans
- Update Security Policies
- Security Training & Awareness

Integrated Security Framework



What Is Your Strategy?

“The true organization is so prepared for battle that battle has been rendered unnecessary.”

“Much strategy prevails over little strategy, so those with no strategy cannot but be defeated (defenses penetrated). Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.”

Sun Tzu
The Art of War

Critical for organizations to seriously develop their strategy first, then execute.

Critical Steps

ecfirst.com

Thank You!

For a complimentary **quick reference card** on ISO 27002, email your testimonial to:

E: **Pabrai@ecfirst.com**

P: 949.260.2030

ecfirst.com

References & Further Reading

Information Security Special Publications (NIST site)
http://csrc.nist.gov/publications/PubsSPs.html
Compliance Portal (ecfirst.com site)
www.ecfirst.com/complianceportal

Books - Pabrai's All Time Favorites

Good to Great, Jim Collins

Built to Last, Jim Collins

The Elephant and the Dragon: The Rise of India and China and What It Means For All of Us, Robyn Meredith

Chasing Life: New Discoveries in the Search for Immortality to Help You Age Less Today, Dr. Sanjay Gupta

Better: A Surgeon's Notes on Performance, Dr. Atul Gawande

Complications: A Surgeon's Notes on an Imperfect Science, Dr. Atul Gawande

The World is Flat, Thomas L. Friedman

ecfirst.com