HIPAA Compliance: How Do We Get There?

A Standardized Framework for Enabling Healthcare Information Security & Privacy

Agenda

- Introduction
- Objectives
- Standardized Framework
- Evaluation & Findings
  - HIMSS 6 Healthcare System
- Conclusion

HIPAA Importance

- Privacy and Security for patient data
- Improved care delivery through coordination
  - Medical history available on-demand for providers
  - Quicker, more accurate eligibility verification for payers
  - Better customer service, better care for patients
- Minimize fraud, inaccuracy in reporting, redundancy of record-keeping

HIPAA Compliance

- Law enacted in 1996
  - Final Draft of Privacy Rule published in 2000, compliance projected by 2003
  - Final Draft of Security Rule published in 2002, compliance projected by 2005
- Are we there yet?
  - Industry compliance = 95% for Privacy, 72% for Security

HIPAA Compliance

- Why is it taking so long?
  - Law provides a destination but no map to get there
  - Everyone is on their own, preverbal 'wheel' is being invented again and again
  - Cost to implement multiplying = over 10x initial projections

Objectives

Primary

- Creation of a standardized healthcare information security guideline for HIPAA compliance
- Allow organizations to leverage roadmap to save time, money, and resources while achieving HIPAA compliance

Objectives

Ancillary

- A suite of security testing tools for assessment and ongoing compliance
- The development of security awareness training procedures and manuals (administrative, functional, and technical)

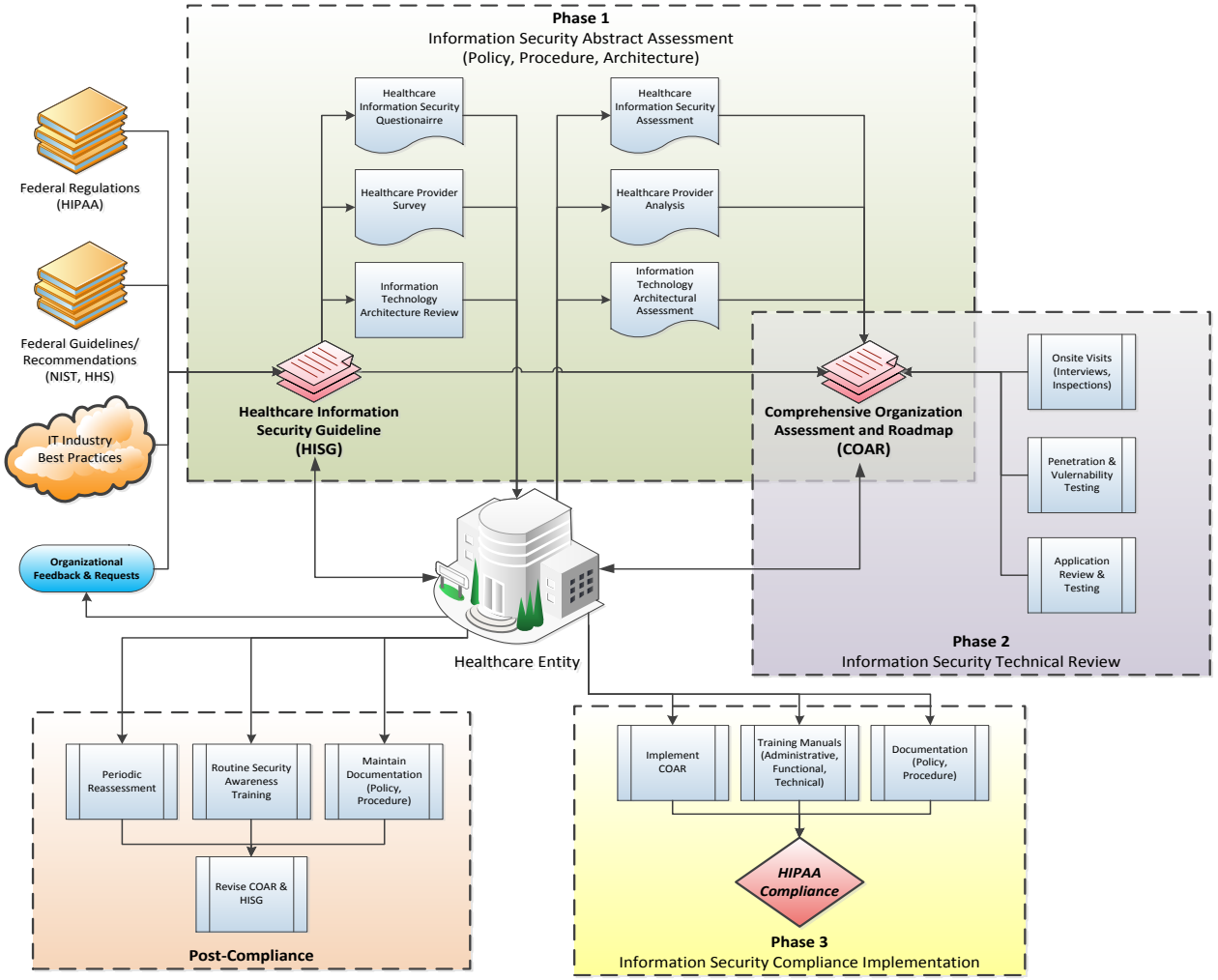
Project Deliverables

- HIPAA Compliance
- Information Security Guideline
- Comprehensive IS Assessment
- Complete Technical Examination
- Training Manuals
- Organizational Documentation

Standardized HIPAA Roadmap

- Creation of the Security Guideline
- Abstract Assessment of the Organization
- Technical Examination of the Organization
- Compliance Implementation
- Maintaining Compliance

Project Framework



Part 1: Security Assessment

- Information Security Questionnaire
  - Completed by IT Staff for 4 key areas – Network, Database, Applications, Infrastructure
- Provider Surveys
  - 25 questions to evaluate Human-Computer Interaction
- IT Architectural Review
  - Network diagrams, data center diagrams, configurations of network devices

Part 2: Technical Evaluation

- Onsite inspections, interviews
  - Examine physical safeguards, interview healthcare personnel, review configurations with IT staff
- Penetration and Vulnerability Testing
  - Validate reported state is actual state of security, test systems/network/applications for vulnerabilities
- Application Review and Testing
  - Document and categorize all applications, examine duplicate uses, evaluate security effectiveness of HIPAA relevant apps

Compliance Implementation

- Create Implementation Plan
- Execute Implementation Plan
- Documentation (Policy, Procedure, Practice)
- Training Manuals
  - Administrative
  - Technical
  - Functional

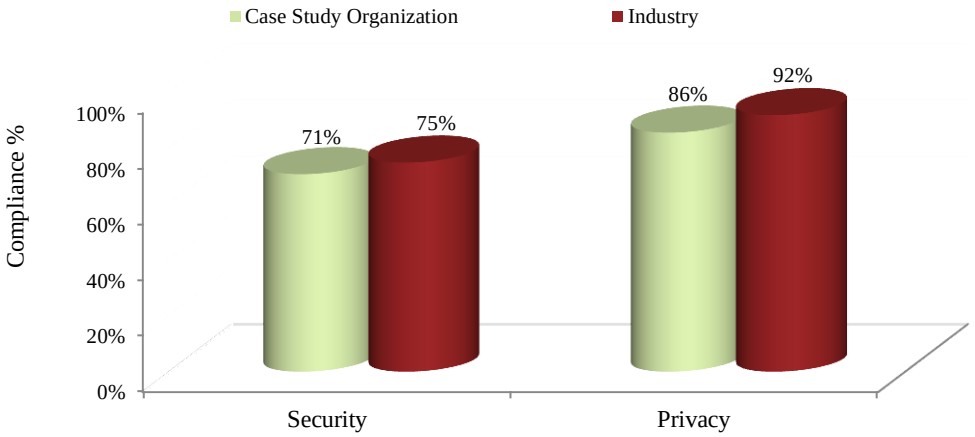
Compliance Maintanence

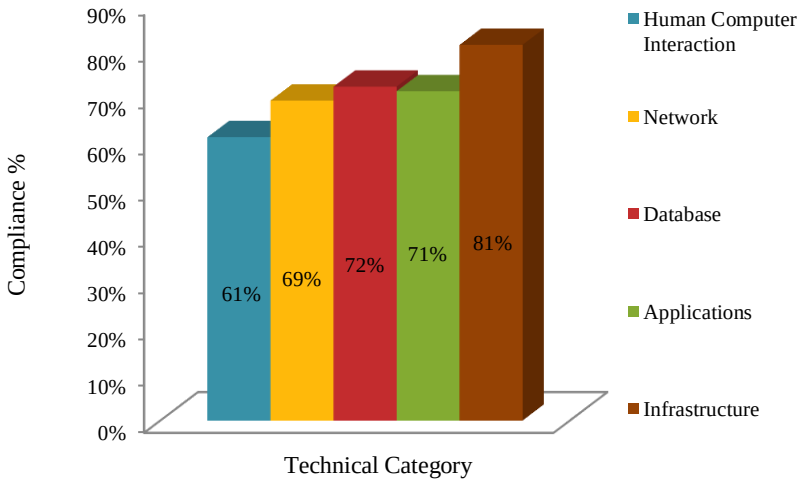
- Periodic Reassessment
- Routine Security Awareness Training
- Maintain Documentation
- Revise Information Security Guideline as technologies evolve/emerge

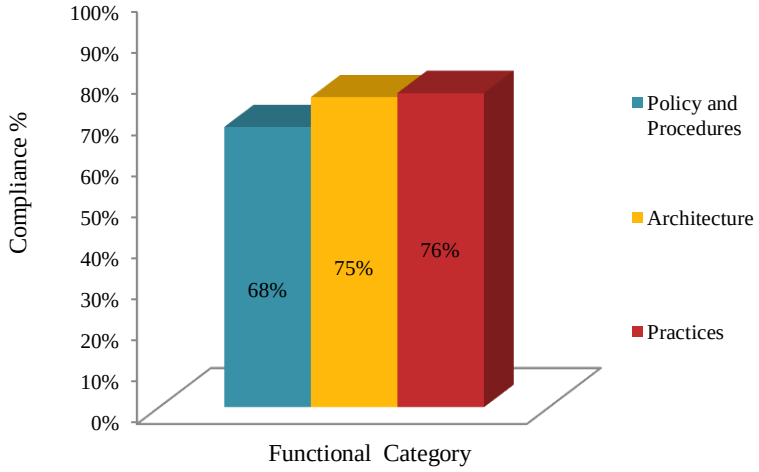
Evaluation

- Evaluation of the proposed research on a typical HIMSS 6 healthcare organization, including partnering hospitals and clinical practices
  - Collaboration in second year of 3 year engagement
  - Phase 1 is complete, findings reported and accepted by organization
  - Phase 2 underway, penetration testing environment being built

Project Findings







Conclusion

- HIPAA compliance is mandatory, organizations have to figure out how to get there and stay there
- Regulations and high-level recommendations exist, but no practical implementation guidance
- This research bridges the wide gap to implementation and will save organizations time, money, and resources

Questions?

Project Director: Dr. Subrata Acharya
sacharya@towson.edu
Doctoral Student: Brian Coats
bcoats1@students.towson.edu