Are You Ready for the April 21 HIPAA Deadline?

Ram Dantu
University of North Texas

Security at UNT

- Computer security certification
- National center for academic excellence
- Certified by NSA and dept of homeland security
- Security LAB
- Research

Security and PACS

- 2 day training seminars UNT/OTech
- 2nd day hands-on
- Network monitoring
- Security experiments

Are Hospitals Ready for HIPAA?

- Survey performed of more than 50 hospitals
- Topological problems:
  - Where to put firewalls?
  - No clearly identified DMZ's
- Firewalls:
  - Lack of internal firewalls
  - Serious threat from inside
  - Service engineers have own laptops (potential threat)
  - Protection of RIS-HIS-modalities is needed

PACS Threats

- Check physically for people that come in
- Firewalls ER-radiology and ER-RIS/HIS

- VLAN's:
  - Segment networks e.g. modalities, HIS, outpatient clinics
  - VLAN works with tags: drop beyond reach of segment

Intrusion Detection Systems

- Only 50% of institutions have IDS
- Limited protection: IDS might not detect application level signatures (DICOM/HL7)

Service Access

- Remote access is typical
- Joint activity by NEMA to develop guidelines
- Central gateway is critical
- Some institutions still allow dial-up access!
- 70% has either one or more Gateways
- Uniformity is highly recommended for audit trail tracking

Workstation Access

- 50% allows Internet access from workstations
- Every connection should go through firewall and IDS

OS Patches: Yes or No?

- PACS is a critical application
  - If Patch: do applications still work?
  - If NO Patch: security vulnerability!
- FDA is issuing guidelines to make vendors react timely
- Vendors might release patches not until months later
- Attacks might come within weeks-days
- Risk management is critical
- Require vendor commitment in requisition for timely availability of patches.

VPN Set-up: SSL vs IPsec?

- NO competing technologies
- IPsec serves from site-to-site: institution to institution
- Mobile applications use SSL (application level)
- Physicians use IPsec for imaging, for secure “pipe” use SSL

Top Three Vulnerabilities

- Risk analysis is critical:
  - Attack paths
  - Protect critical resources
- Segment using VLANS
- Use internal firewalls
- Use centralized gateway for remote service access