Briefing: The Information Assurance Universe from a Private Practice Perspective

18 September 2015

Guy Wassertzug, President/CEO
Brett Bonifant, COO

About:

FNA P.C.
a Neonatal & Pediatric Subspecialty Group

Fairfax Neonatal Associates
Neonatology & Hospitalist Pediatrics

The Pediatric Lung Center
Pediatric Pulmonology, Allergy & Immunology, Sleep Medicine

Pediatric Surgical Group
Pediatric Surgery

Pediatric Infectious Disease Group
Pediatric Infectious Disease

The Maggie Foundation
for the Premature and Pediatric Subspecialty Patient

Management Consultants for Affiliated Physicians, Inc.
a business subsidiary of FNA, P.C.

- NICU:
  - Started NICU at INOVA Fairfax Hospital 40 Years ago.
  - Also Operating NICUs at Inova Fair Oaks and Inova Loudoun Hospitals.
  - Service Needs of 20,000 Newborns Annually
- Other Subspecialties:
  - Pediatric Surgery
  - Pulmonology/Allergy/Immunology/Sleep Medicine
  - Hospital Pediatrics
  - Infectious Disease

About: InfoStructures — Better Networks®

- Facilities Management: Data Center Operations, Server/Client Management, NOC Ops, Network Support, Service Desk/End User Support, Comprehensive Managed Services & Hosting

- Systems Architecture & Deployment: Enterprise Network/Data Center Design and Deployment

- Information Assurance/Network Security: COOP, System and Network Security Device and Application Configuration, CERT Resources

- Software Development

- Governance/Compliance: HIPAA, PCI

- Industries: Health Care, Finance, NonProfit, FedGov

- Founded: 1988 (27 years)
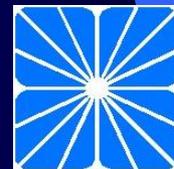
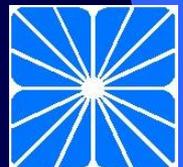# CyberSecurity: The Threat

- Nature of the Threat:
    - Constant – the Internet is always on
    - Outsiders – criminal enterprise; state and non-state actors
    - Insiders – innocent and malicious users
- Confronting the Threat:
    - An integrated, comprehensive security approach
    - Incorporated into every IT-related business decision - not "bolted on"
- Breaches are Expensive!:
    - 2015 IBM/Ponemon Data Breach Study: Cost of a Health Care Data Breach is $363 per Record (http://www-03.ibm.com/security/data-breach/)

The Information Assurance "Universe"

- Compliance
- Human Resources
- Activities/ Procedures
- Tools/ Resources
- Governance/ Policy
- Information Assurance/ Cybersecurity

Focus:

Information Assurance/ Cybersecurity

Human Resources

- Designate a Security Officer (ISSO):
  - Guides Policy
  - Shapes Security Posture
  - "Executor" of Information Assurance Activities
- Identify Consultants/Specialists:
  - Policy
  - Architecture
  - Deployment/Implementation
  - Support
  - Auditing
  - Legal
  - Breach Assessment/Response

Focus: Information Assurance/Cybersecurity — Activities/Procedures

- Technical IA Activities:
  - Proactive patching
  - Log Review/Monitoring, Including Privileged Users
  - Tool tweaking and log review
  - Maintain Incident Response Plan
  - Change Control
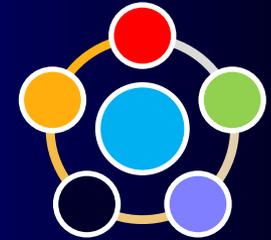 - COOP/DR Planning and Testing

- Non-Technical IA Activities:
  - Regularly Scheduled User Training (Web hygiene, Phishing, Social Engineering)
  - Maintain Incident Response Plan
  - Developing, Integrating and Evangelizing Best Practices

Focus:

Information Assurance/ Cybersecurity

Activities/ Procedures

BREACH!:

- Engage Experts (Security, Legal, Insurance, Partners, Law Enforcement)
- Evaluate Data Loss
- Isolate Networks/Systems
- Identify Breach Sources & Methods
- Review Logs/Backups
- Notify Affected Parties
- Design and Implement Remediation/Recovery Procedures

Focus:

**Information Assurance/ Cybersecurity**

Tools/ Resources

Tools/Resources:

– Premises Based/Outsourced/Hybrid

– Filtering/Reputation Services (Web, Email)

– Data Loss Protection via Firewalls and Other Products

– Policy-based HIPAA Enforcement Tools

- Email – "Trust but Verify"
- Secure Mobile Applications

– Mobile Device Management for Phones, Tablets, Laptops

– Encryption

– Automated Training/User Evaluation Tools
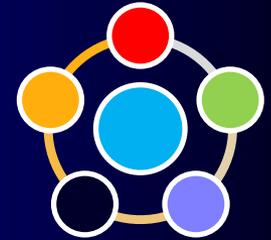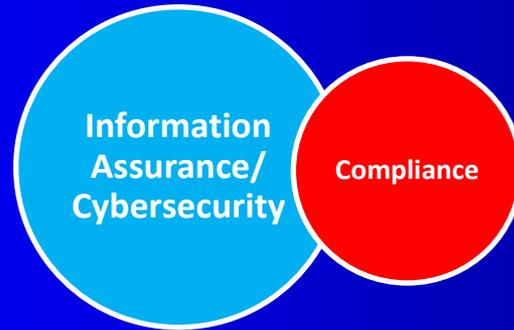
– Dual Factor Authentication (2FA)

Focus:

Information Assurance/ Cybersecurity
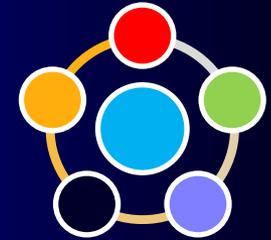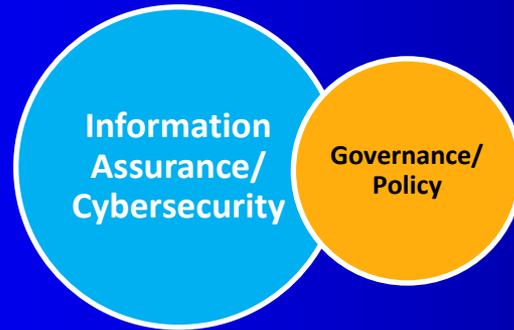
Governance/ Policy

Governance/Policy:

– Acceptable Use Policy (AUP)

– Bring Your Own Device (BYOD) Policy

– Privacy Practices

Focus:

Information Assurance/ Cybersecurity

Compliance

Compliance:

- HIPAA/HITECH Act: No Certification but Established Audit Standards Exist

- PCI: Graduated Compliance Requirements Based on CC Transaction Volume

Discussion/Questions: