Healthcare Security Professional Roundtable

The Eighth National HIPAA Summit

Monday, March 8, 2004

Panelists

- **John Parmigiani, Sr.VP for Consulting Services, QuickCompliance, Inc.; President, John C. Parmigiani and Associates, LLC (moderator)**
- **Ali Pabrai, CEO, HIPAA Academy**
- **Tom Walsh, President, Tom Walsh Consulting**
- **Chris Apgar, Data Security and HIPAA Compliance Officer, Providence Health Plan**
- **Tom Welch, CEO, Secure Enterprise Solutions**
- **Bob Tahmaseb, Principal Systems Engineer, RSA Security**

John Parmigiani

Sr. VP for Consulting Services
QuickCompliance, Inc.
and
President
John C. Parmigiani and Associates, LLC
Ellicott City, MD

Action Items for Compliance

- **Read and understand the Rule**
- **Appoint a CSO/HIPAA Security Team**
- **Determine ePHI data flow and existence in information systems**
- **Conduct a risk analysis- assets, vulnerabilities, threats, impacts**
- **Examine, update, and create security policies and procedures in line with the implementation specifications**
- **Work with your vendors and business associates to enlist their help**

Action Items for Compliance

- **Identify existing security safeguards- administrative, physical, and technical**
- **Build and deliver security training programs**
- **Identify and prioritize remediation projects**
- **Build an ongoing risk management process**
- **Create a security management process with accompanying documentation that supports your decision making/choices relative to the security standards**
- **Stay on top of "best practices" within the healthcare industry and federal guidance**

Uday O. Ali Pabrai, CISSP, CHSS

Chief Executive

HIPAA Academy

Warrenville, IL

Seven Steps to HIPAA Security Compliance

HIPAA Security Rule

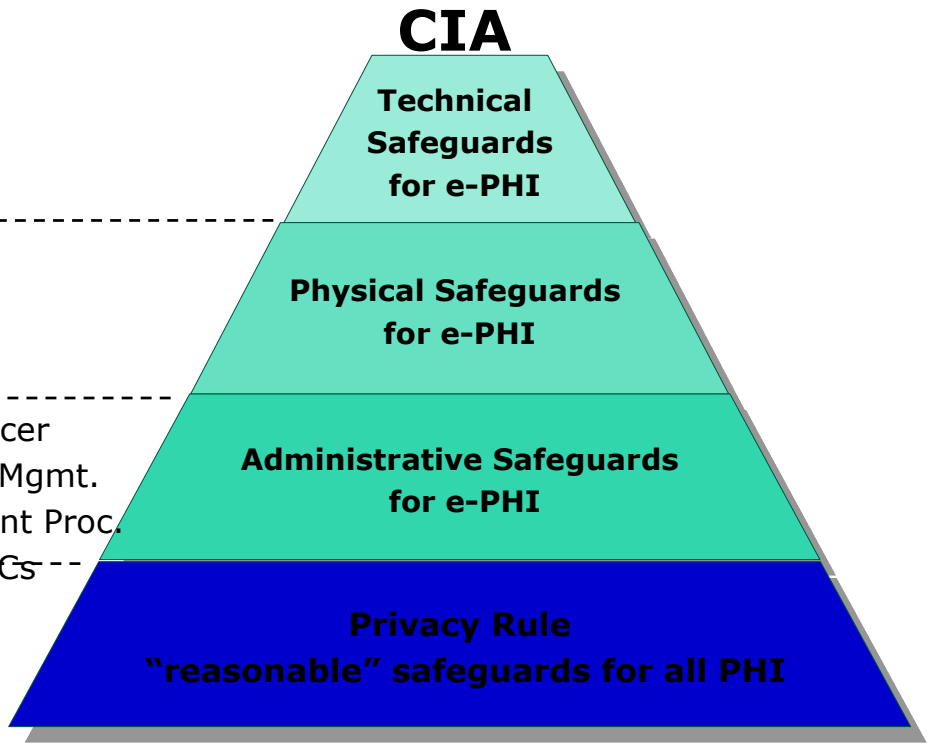
- Access Control
- Audit Control
- Integrity
- Person or Entity Authentication

- Transmission Security
- Facility Access Controls
- Workstation Use
- Workstation Security

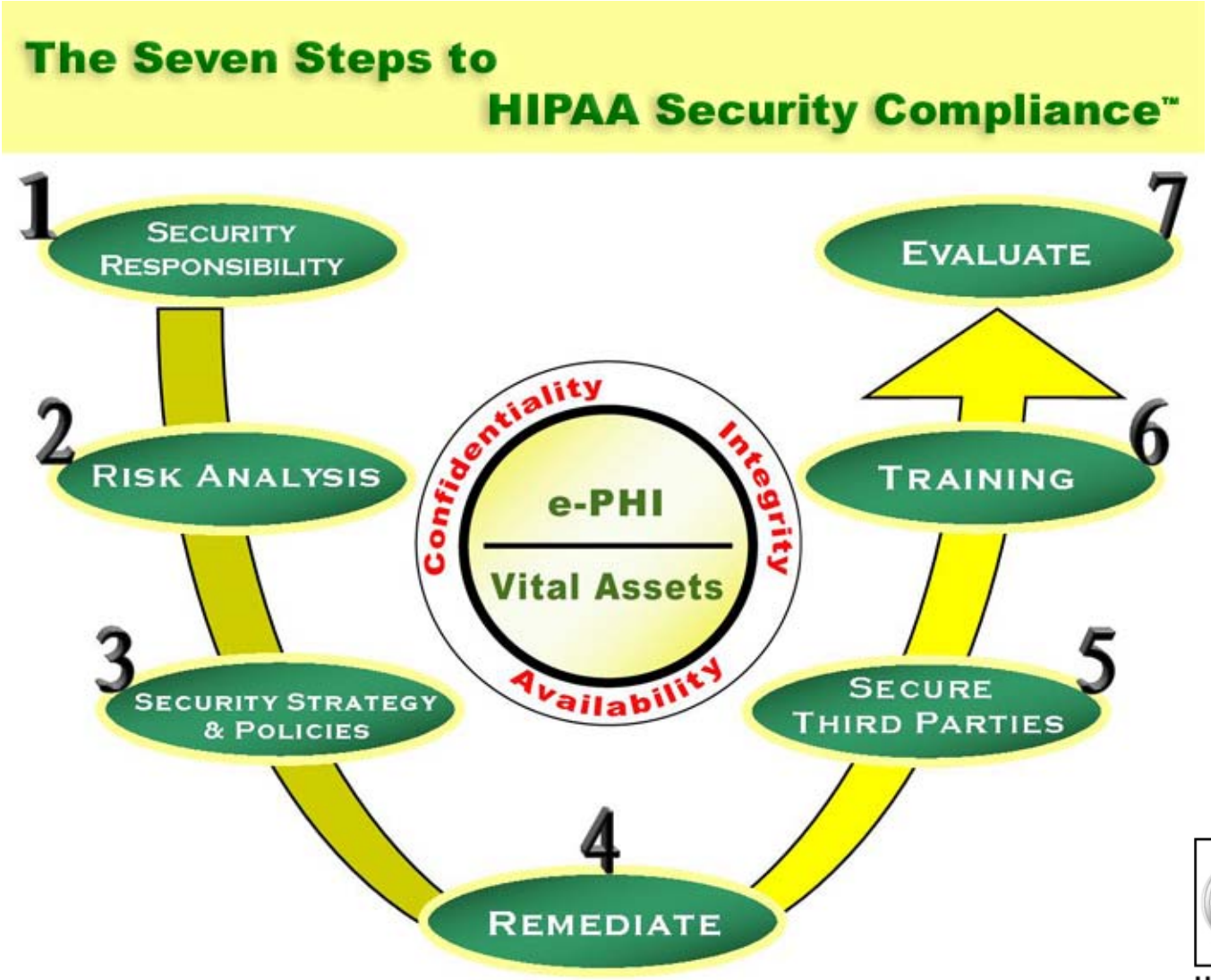
- Device & Media Controls

- Security Mgmt. Process, Sec. Officer
- Workforce Security, Info. Access Mgmt.
- Security Training, Security Incident Proc.

- Contingency Plan, Evaluation, BACs



HIPAAShield™ Methodology



HIPAA Academy™
HIPAAacademy.Net

Tom Walsh, CISSP

President

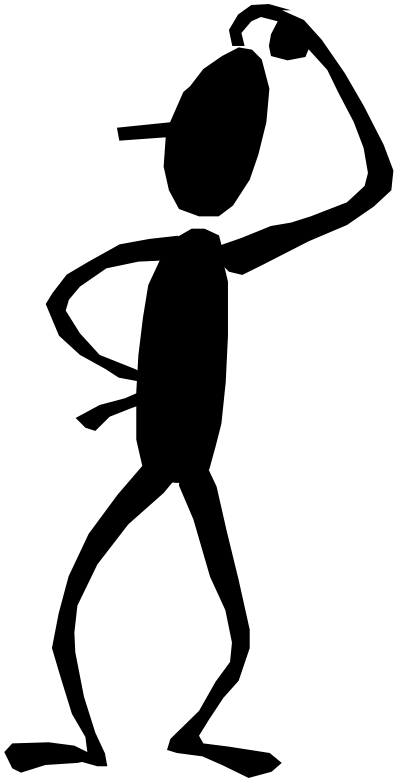
Tom Walsh Consulting, LLC
Overland Park, KS

Risk Profiling

- **What is it?**
- **How does this help with risk analysis?**

<u>Example:</u>

Car Insurance



Traditional Approach to Assessing Systems (Ref: NIST SP800-26)

Major App 1

Data

Application

Interfaces

Network

Hardware & Operating System

Physical/ Environment

Operational Practices

Assessing Controls

Major App 2

Data

Application

Interfaces

Network

Hardware & Operating System

Physical/ Environment

Operational Practices

Assessing Controls

Risk Profile Approach

Major App 1	Major App 2	
Data Application Assessing	Data Application Assessing	*A hierarchical approach to assessing controls and risks*
Interfaces	Interfaces	Risk Profile
Network	Network	Risk Profile
Hardware & Operating System	Hardware & Operating System	Risk Profile
Physical/ Environment	Physical/ Environment	Risk Profile
Operational Practices	Operational Practices	Risk Profile

Chris Apgar, CISSP

Data Security and HIPAA Compliance Officer

Providence Health Plan

Beaverton, OR

Audit – Implementation is only the Beginning

- **Security audit, like financial audit good business practice**
- **Audit program should be designed to:**
  - **Keep the masses honest**
  - **Monitor potential vulnerabilities**
  - **Be thorough without being onerous**

Audit – Implementation is only the Beginning

- **Sized to fit the organization, technical configuration & business**
- **Should include regular and random audits and audits when major changes occur (i.e., new technology, high level staff leave, etc.)**
- **Need to publicize and follow through**

Evaluation

- **Evaluation on going**
- **Healthcare – an ever changing environment while audits and risk assessments are snapshots in time**
- **What was an effective audit process, security practice, etc. yesterday may not be today**
- **Embed in culture, planning and processes**

Thomas Welch, CPP,CISSP

Chief Executive Officer

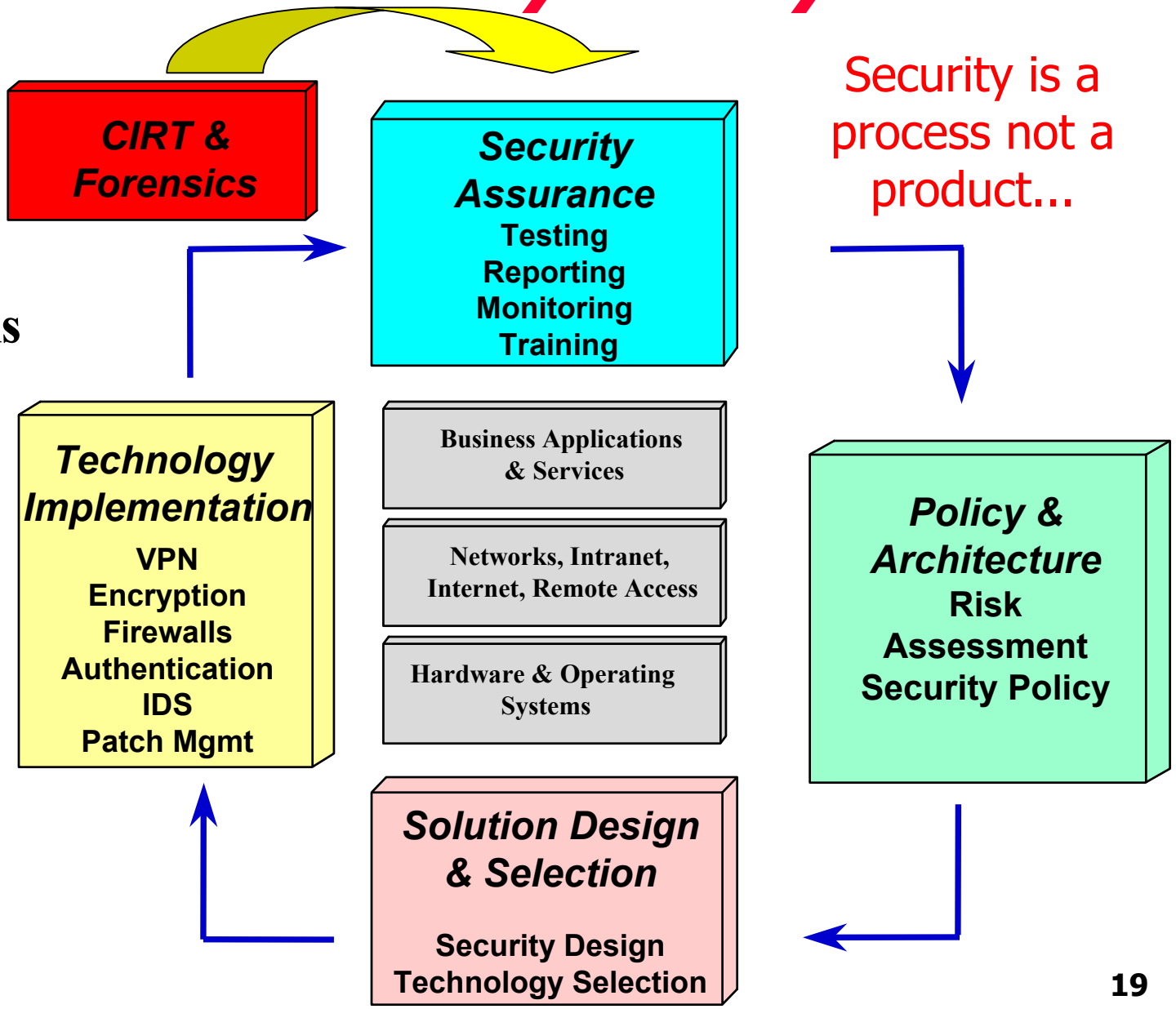
Secure Enterprise Solutions, Inc.
Parsippany, NJ

Information Security Lifecycle

Security is a process not a product...

Building Blocks

- People
- Process
- Technology



Information Security Policy

- **Provides the foundation for the information security program**
- **Puts employees and consultants on notice pertaining to issues of:**
  - **Acceptable use of IT resources**
  - **Employee Monitoring**
  - **General security requirements**

Information Security Policy

- HR Policies
  - **Monitoring Awareness**
  - **Privacy Issues & 1st Amendment Rights**
  - **Company Equipment Use**
  - **Who Owns the Data**
- Operational Policies
  - **Internet & Intranet Usage**
  - **Passwords**
  - **E-mail usage**
  - **File transfers & Attachments**
  - **Virus Control**
  - **Data Classification Sensitivity**
- Moral & Ethical Conduct
  - **Etiquette and Proper Usage**
  - **Pornography**
  - **Harassment**
- Legal Responsibilities, Penalties & Enforcement
  - **Warning Notice**
  - **Incident Response Plan**

InfoSec Awareness

- **Policies provide the notice and guidelines, while awareness training provides the knowledge**
  - **Can be classroom-based or CBT-based**
  - **An on-going program is more effective that a one-time course**
    - **E-mail alerts, bulletins, reward programs, posters, etc.**
  - **Goal is to change behavior**

Bob Tamaseb

Principal Systems Engineer

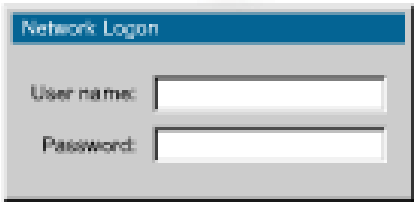
RSA Security, Inc.
Bedford, MA

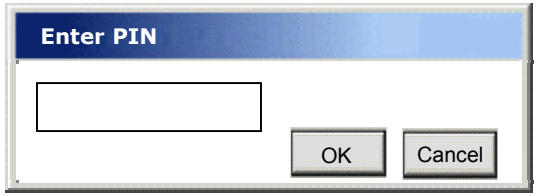
HIPAA Authentication: Proving Your Identity

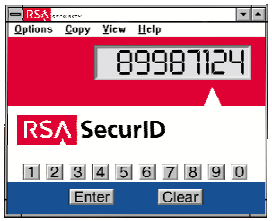
- Physical vs. Digital Identity
- Technical Safeguards for person and entity authentication
- Types of Authentication
  - Something you know
  - Something you have
  - Something you are
- Leveraging authentication for access management

Types of Authentication

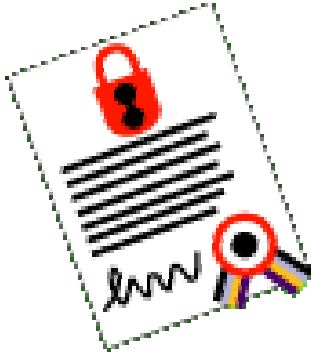
Something you know







Something you have



Something you are

Thank You

Questions?