Security Design
INTERNATIONAL™

HIPAA Security:
Gap Analysis, Vulnerability Assessments, and Countermeasures

Don Hewitt and Chris Goggans

March 1, 2001

Agenda

- The Proposed Rule
- The Gap(s)
- A Network Security Primer
- Vulnerability Assessments
- Real Examples
- Countermeasures

Information Security – Classical Definition

- Confidentiality
- Integrity
- Availability

Some Characteristics of the Rule

- Technology neutral
- Deliberately general guidance
- Extremely broad applicability
- An attempt at scalability
  - Easier said than done
  - Serious technical issue

Proposed Security Requirements

- **Administrative procedures…**
- **Physical safeguards…**
- **Technical security services…**
- **Technical security mechanisms**

"The standard does not address the extent to which a particular entity should implement the specific features. Instead, we would require that each affected entity assess its own security needs and risks and devise, implement, and maintain appropriate security to address its business requirements." Federal Register, August 12, 1998 [43250]

Gap Analysis

- Applicable to any aspect of the rule…
- Determine the “gap” between where you are, and where you need to be.
- One such gap will be defined by your network security posture.

Other Gaps of Interest…

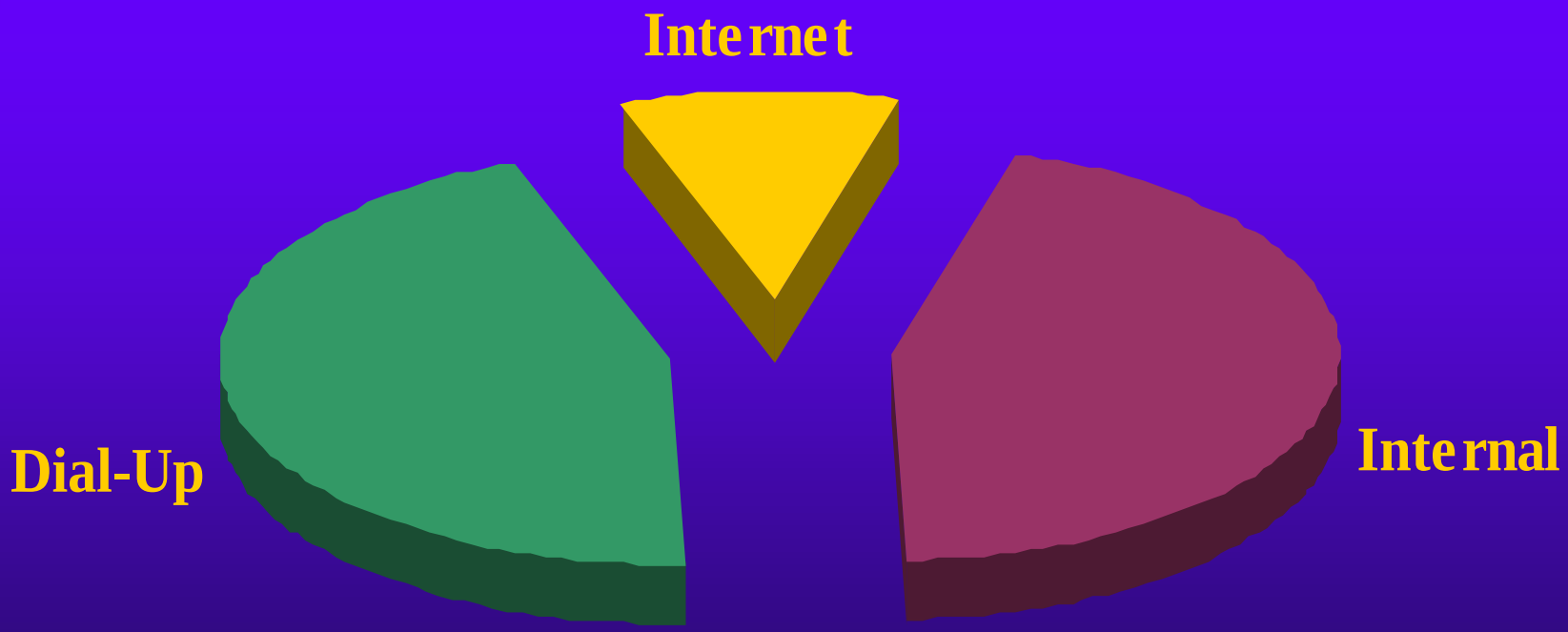
- **Budget Gap**
  - **Between what you have and what you need to implement HIPAA**
- **Knowledge Gap**
  - **Between what you know about information security and what you need to know to implement HIPAA**
- **Practicality Gap**
  - **Between HIPAA as currently formulated and the medical/business processes necessary to deliver health care**

“Honor the Threat”

- Threats are both internal and external.
- Increased Connectivity = Increased Risk
  - Internet
  - Other networks
  - Dial-up connections
- Threats are both technical and physical.
- In early 2000, a report by CSI and the FBI stated that 90% of 650 corporations interviewed had detected attacks in 1999.

Network Threat: Perception

Network Threat: Reality



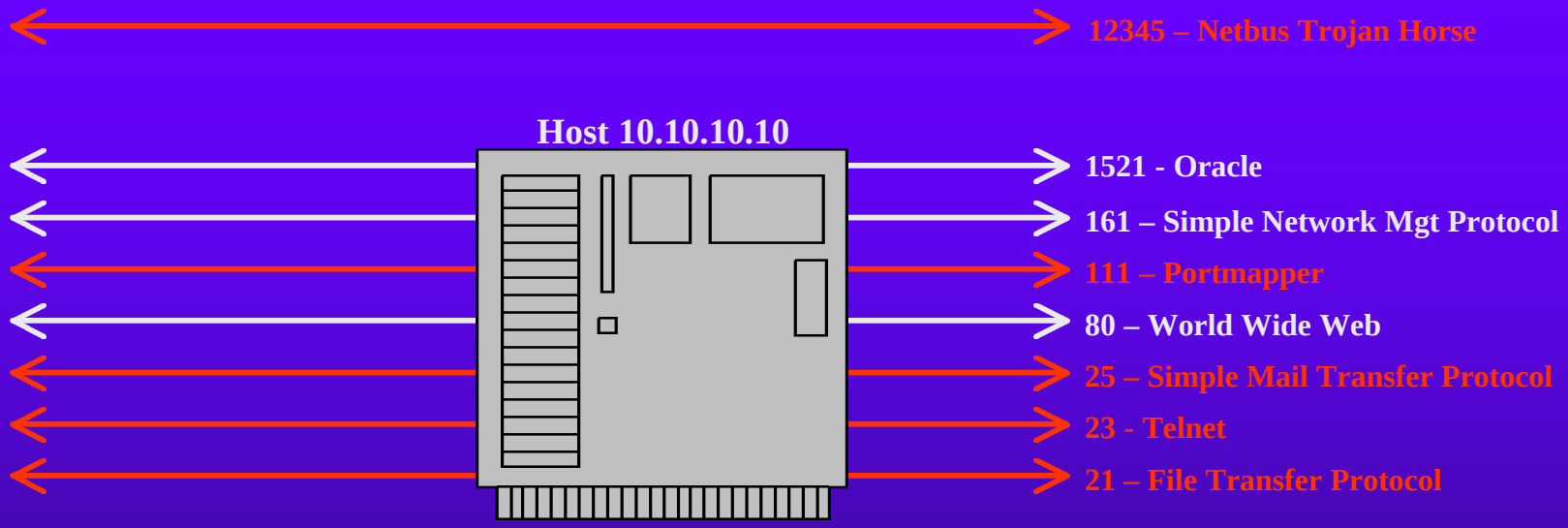
Evolution of Workstation Connectivity

- Standalone personal computers
- Local Area Network connects small workgroups
- Larger LANs and client server software provide distributed services and applications
- Wide Area Networks connect LANs to offer enterprise-wide connectivity
- The Internet allows enterprises and individuals to connect directly to millions of known and unknown individuals world-wide

TCP/IP – Enabling the Internet

- Transmission Control Protocol / Internet Protocol
- Provides a framework for inter-networking and multiple simultaneous communication via standard “packets”
  - Addressing standards allow “routing” of messages across multiple dissimilar networks
  - Layering of communications responsibilities and the concept of “ports” allows diverse systems and applications to communicate

TCP/IP Vulnerabilities



- **Connect to network – 3 desired services**
- **Superfluous services started by default**
- **Over 65,000 ports – first 1024 “reserved” – what else is out there?**

It's All Connected!

- "Ping"
  - See if a host is present on the network
  - First step in mapping network
- "Port Scan"
  - See which port(s) are responding on every host
  - High probability of identifying function by its port number
- "War-Dialing"
  - Consecutive dialing of phone numbers in search of carrier tone

Some Terrible Assumptions

- It's only a workstation.
- No one will "see" a dial-up connection.
- The manufacturer's default settings will be fine.
- It will be ok to connect just this one machine across multiple networks for ease of use.

e-Liable

- Direct Liability – First Party Information
  - Proprietary data and intellectual property
- Direct Liability – Third Party Information
  - HIPAA
  - Gramm-Leach-Bliley Act
- Indirect Liability
  - As a conduit (through unprotected connections)
  - As a platform (allowing use of resources as attack platforms, e.g., in a DDOS)

The Inevitable Conclusion…

It’s not about perfect security;

it’s about DUE DILIGENCE.

"Given the inevitability of computer losses, you’ll be judged not by whether you were the victim of an attack, but by how well you planned for it."

- Computer Security Institute

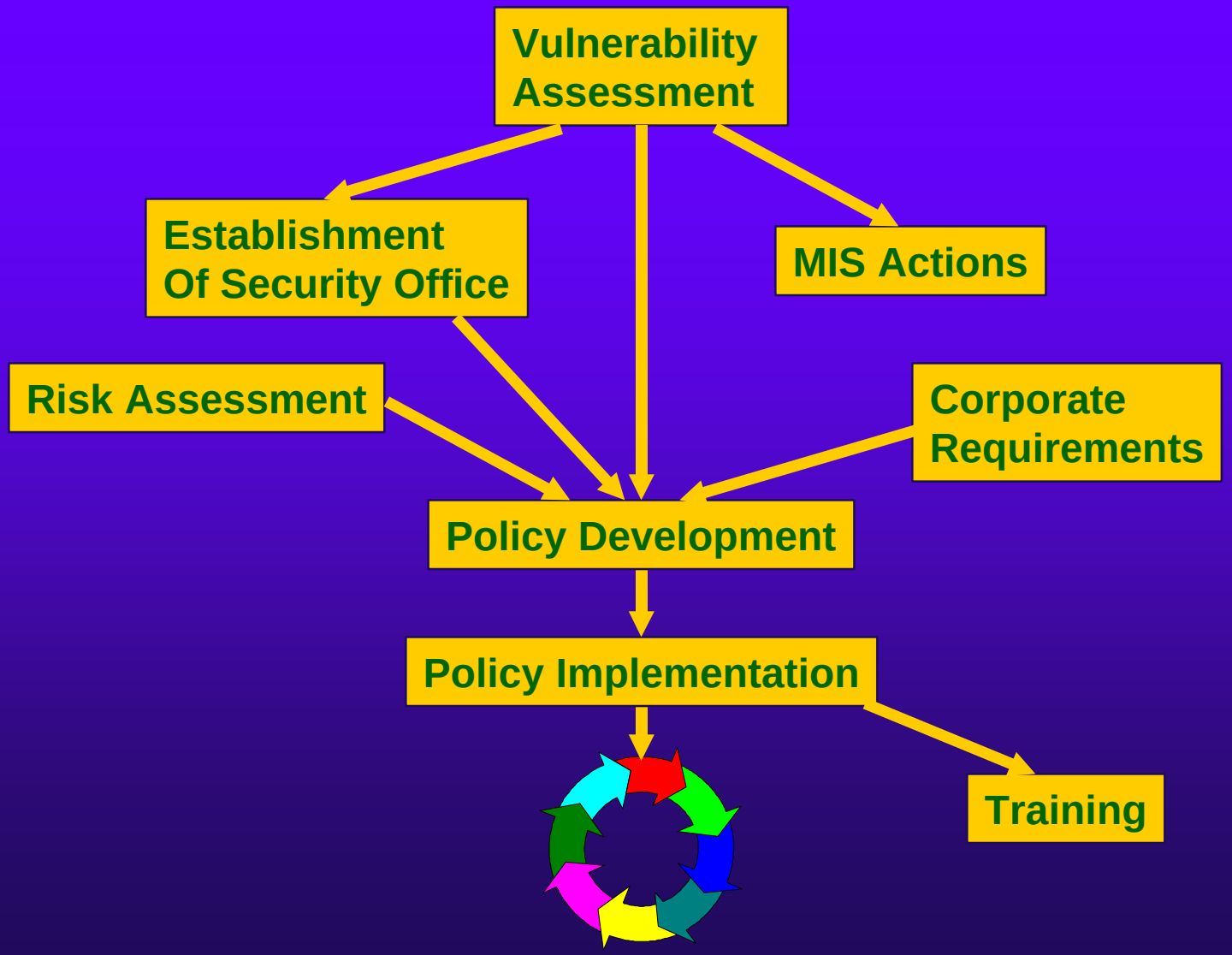
Vulnerability Assessments

- Internal and external attack
- Validation of existing security mechanisms
- Detailed analysis of networked devices and services
- Audit for policy compliance
- Prioritized recommendations for improving security posture

WHY Vulnerability Assessments?

- Only realistic way to determine vulnerabilities
- Get a baseline of vulnerability state
- Prioritize remedial actions
- Correct serious problems quickly
- Assure that policies address real vulnerabilities
- Evolving best practice

Assessments as Program Drivers



News Flash – and possible heresy…

Healthcare network security concerns are not significantly different from other industries!

Real Examples: Large University Hospital

- Only router filters separated the two environments
- Extensive inter-entity traffic
- Broadcast networks on both sides allowed “sniffing” of passwords
- Poor password choices on both sides
- Similar accounts on Netware, Unix, and Mainframes

Real Examples: Cardiac Care Center

- No Internet firewall
- Open (unpassworded) dial-up connections
- Vulnerable single-sign-on server led to compromise of Netware, Unix, and Tandem accounts (including active patient data)

Real Examples: Insurance

- Customer had a very small Internet presence (16 IP address allocation, only live hosts were mail server and firewall)
- Customer users made posts to USENET news and common mailing lists
- Firewall allowed incoming authentication and gave different error messages for valid and invalid users
- POP server did not log failed login attempts

Real Examples: Telecommunications

- Large US telephone company
- Dial-ups found with unpassworded pcAnywhere
- pcAnywhere system used primarily for access into security camera monitoring
- Full access to internal network, including switching systems, billing, etc.

Real Examples: Public Utilities

- Large power generation company
- Unpassworded modem dial-ups found less than a dozen phone numbers away from main number
- Many administrator level accounts on main NT server with password of “password”
- Accounts on VMS nuclear power monitoring systems found with no password

Real Examples: Manufacturing

- Customer had large Internet-accessible network, but made good use of firewall products and used internal-use-only addressing
- Customer had multiple hosts dual-homed to internal network on the DMZ (other than the firewall)
- Customer had extensive unprotected connectivity to business partners

Common Problems UNIX

- Ubiquitous default accounts and passwords
- Open NFS exports
- Poor trust relationships
- Open X-Windows servers

Common Problems Windows NT

- Null Session access almost always enabled
- Poor passwords choices endemic even on administrator-level accounts leading to password database (SAM) access
- Shared drives found with no passwords

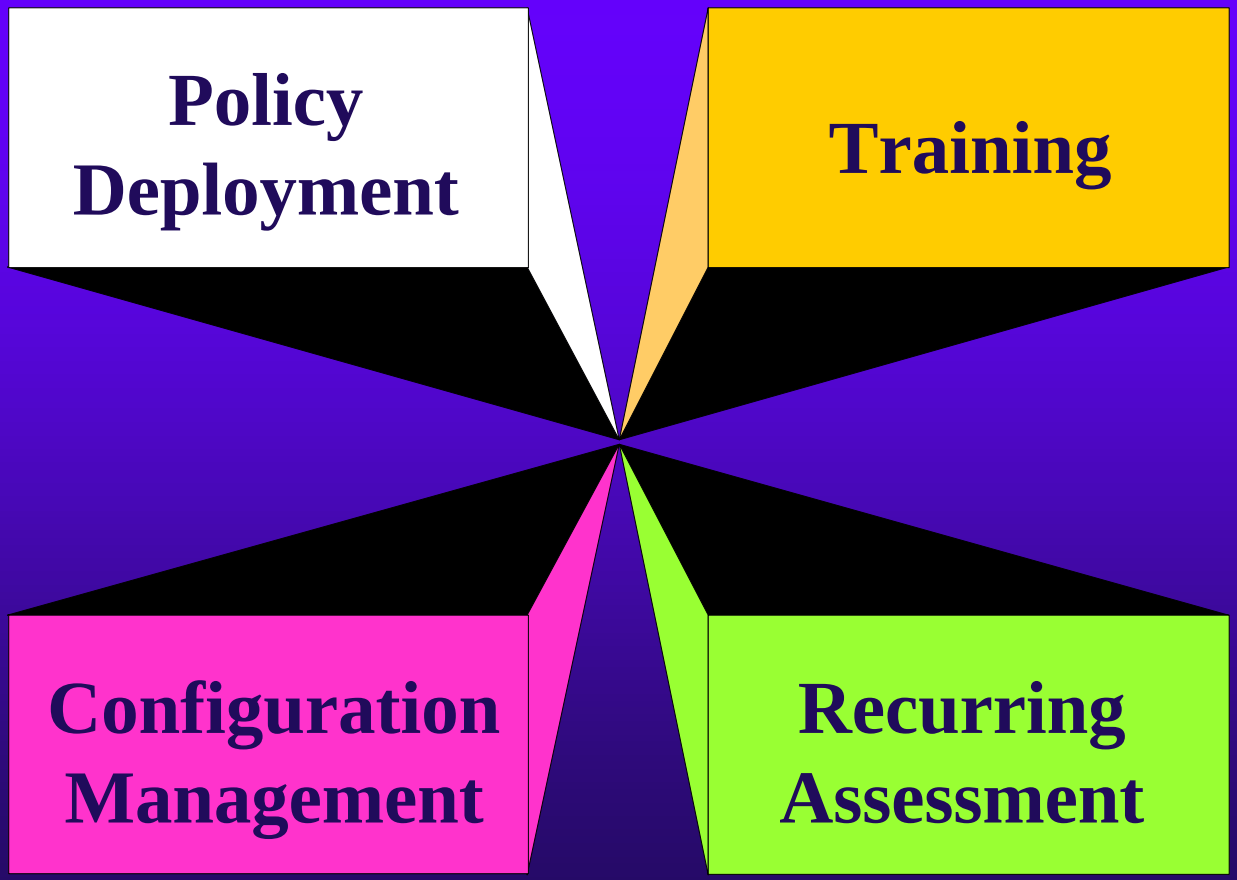
Common Problems Generic

- The Internet is usually very easy to secure, but *modems* (authorized and unauthorized) are the number one entry mechanism to a company's network
- *Poor passwords* are the number one mechanism to gain host-level access
- *Non-switched networks* are still everywhere allowing network "sniffing"

Countermeasures: Searching for the Silver Bullet

- Scanning tools
- Network firewalls
- Intrusion detection
- Virtual Private Networks (VPN)
- Encryption

Emerging Best Practice – A Formal Security Program



Emerging Best Practice – A Formal Security Program

- MANAGEMENT SUPPORT
- Target critical areas
  - Permitted use
  - Passwords
  - Connectivity
  - Incident Response
- Related policies
  - Personnel
  - Physical security
  - Disaster recovery

Emerging Best Practice – A Formal Security Program

- Mandatory awareness training
- Advanced training for administrators
- Publications
- Web page
- Security Awareness Week

Emerging Best Practice – A Formal Security Program

- Standard configurations for servers and workstations
- Process for patches and upgrades
- System enforcement of policies
- Process for virus scanning

Emerging Best Practice – A Formal Security Program

- Recurring internal audits/compliance checks
- Periodic third party vulnerability assessments

Summary

- Increased connectivity – increased risk
- Real liability exists
- Best practice vs perfect security
- Formal security programs needed
  - Scaled to enterprise
  - Oriented to counter threat
  - Continually updated to remain effective
- Security is a process, not a product…