# HIPAA Case Study

## Implementing a Security Program at a Mid-size Hospital

Lehigh Valley Hospital and Health Network
Brian Martin
brian.martin@lvh.com

LEHIGH VALLEY HOSPITAL AND HEALTH NETWORK

# LVHHN

- Medium healthcare organization
  - 700+ licensed beds
  - three hospitals, a cancer center, and a trauma center
  - 20 satellite facilities
  - 1200 member medical staff (250 direct employ)
  - 7000+ active users, 1000 remote
  - 175 servers, 4000 workstations, 25 major systems
  - 15 mile diameter MAN
  - Free standing data center

# Briefing Overview

- Timeline narrative
- Highlights in timelines
- Advice, Comments, Lessons Learned
- New Ground
- Open Discussion

# Timeline Pre-1999

- 1998 Consultants hired to evaluate Internet and Email security
  - So began the list of things “to do”
- Wheel Group Security Penetration Testing
  - Early days, primitive but effective
  - Management began to see there was a need to engage security more actively
- IS Security section consisted of one analyst/supervisor and two specialist clerks.

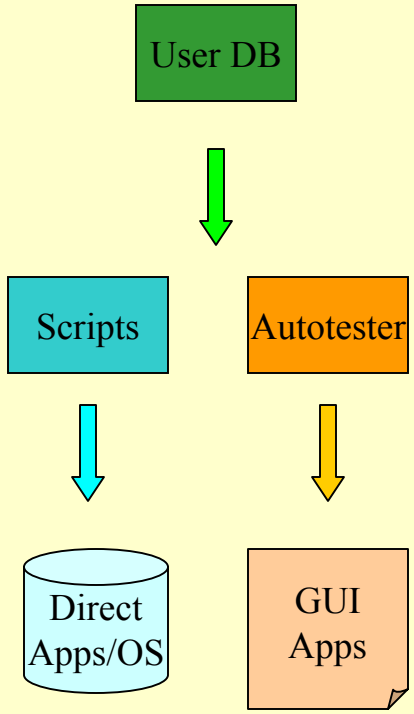
# Timeline 1999

- Company hires consultants to
  - review applications for HIPAA applicability
  - review policies for HIPAA compliance (estimated) and recommend changes
  - Assess the security department operational situation
- Company hires security expert to
  - Head up growing security department technical needs
  - Nurse initial HIPAA security analysis
  - Direct security growth for HIPAA compliance
- Rewards for Rats

# Timeline 2000

- Created and prioritized shopping list of security problems
- Began automation of user authorization procedures
- Began formalization of Application Security Requirements
- Compliance Report on Security Summit Guidelines (Wedi Members)
  - We scored ~10% of the recommended level of readiness
  - No area was within the desired level
- Created security plan based on Response and business factors
- Annual external auditors review security situation
- External auditors contracted to do formal gap analysis
- Firewall Restructuring
- Security moved under CIO

# Automation




- Central User Information Repository
  - Validation/Auth. during data input
- Batch user privilege add/mod/delete
- Fewer errors, faster loads
- Fewer root users
- Audit trail
- Additional programmer requirement
  - Continual maintenance as apps and platforms are upgraded

# Application Security Requirements

- Modified policy, procedure, and acquisition documents
- Increased security influence in purchasing decisions
  - No generic user ID's
  - Granular access control
  - Role based security
  - Audit trails w/ export capability
  - User management interfaces
  - Distributed system administrator privileges
  - Password controls

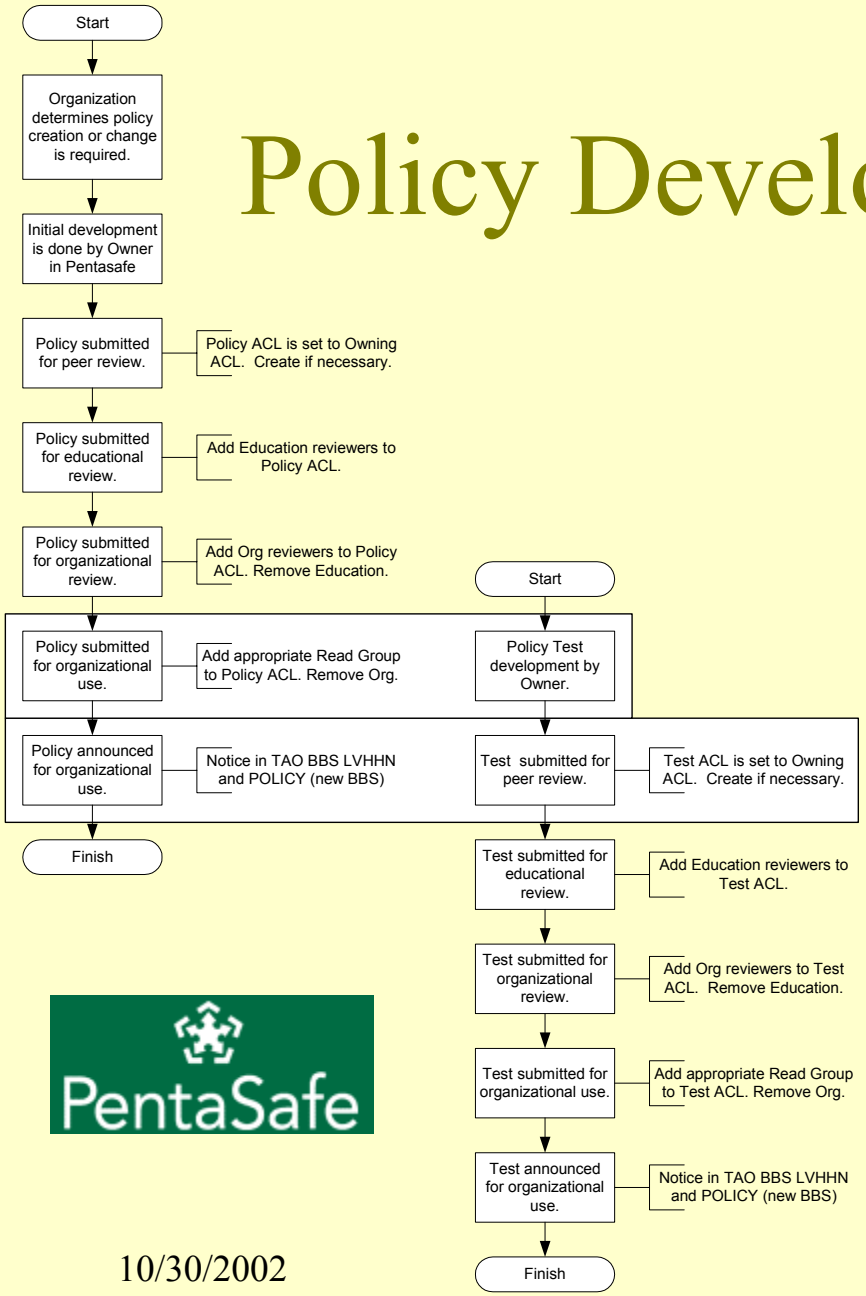
# Timeline 2001

- Annual external auditors review security situation
  - Same list, a few less entries
  - Steady progress results in more wins than dumping money into it
  - Have to have time to integrate into the business
- Updated and improved enterprise virus protection

# Timeline 2002

- Formal Policy Development Process Instituted
- Border Router Assessment using RAT & Others
- Outsourced Intrusion Detection Systems
- Internal Audit confirms security needs
  - Using other parts of the business to see to their own interests is the best way of obtaining funding.
- Personnel reduction
- Firewall/VPN RFI
- End User Education
- Modem/pcAnywhere scan (War-dialing)

# Policy Development Process




- Structure is necessary to:
  - Provide deadlines
  - Establish workflow
  - Explain costs
  - Clarify expectations
  - Create a permanent process
- Using Vigilent Policy Center
  - Policies and Procedures
  - Knowledge Testing
  - Version Control

# Border Patrol


- Hired Stenstrom Scientific to review border router configurations and run simple vulnerability tests
  - Mini Security Review
  - Prioritized and Cost Effective

LEHIGH VALLEY HOSPITAL AND HEALTH NETWORK

# Outsourced IDS

- Intrusion Detection Systems
  - easily encapsulated
  - self contained
  - constantly observed


  - If it can be defined as a separated entity, we outsource it. We *do* maintain internal expertise to understand the situations which develop, but not at a level to support doing IDS ourselves.

# Firewall/VPN RFI

- Used RFI process to get free redesign consulting on Internet connection and products
  - New fault-tolerant design
  - Better growth capacity
  - Better management capabilities
  - Awesome VPN capabilities
    - Custom end user installation programs by Stenstrom Scientific
  - Outsourcing management and maintenance of Checkpoint cluster to Red Siren

# End User Education

- Existing Programs
  - Email propaganda
  - New employee orientation briefing

- New Programs
  - Online HIPAA compliance education
  - Specialized Policy knowledge testing


# War-dialing

- Hired Stenstrom Scientific to call two exchanges (20,000 #'s)
- Locates rebel modems
- Identifies open back doors
- Proven, historical, and now easier means of access

# Timeline 2003 Prediction

- Education restructuring
- Increased user management automation
- Increased monitoring, addition of email filtering
- Consolidation of audit trails for composite views and simplified backup.
- Manpower assistance: hiring two contractors for spot assistance
- Updating Security Documentation and Procedures (succession planning)
- Increase disaster recovery capabilities
- Hard Core Security Evaluation and Penetration Test
- New Single Sign-on Product (CA eTrust)
- Formation of Information Security Council

# How We Decided The Priorities

**Evidenced Way**

- Budget
- Management Input
- Risk Evaluation
- Manning Levels
- Avoid high-risk applications

**Ideal Way**

- Risk Evaluation
- Mitigate high-risk applications
- Management Input & Budget
- Manning

LEHIGH VALLEY HOSPITAL AND HEALTH NETWORK

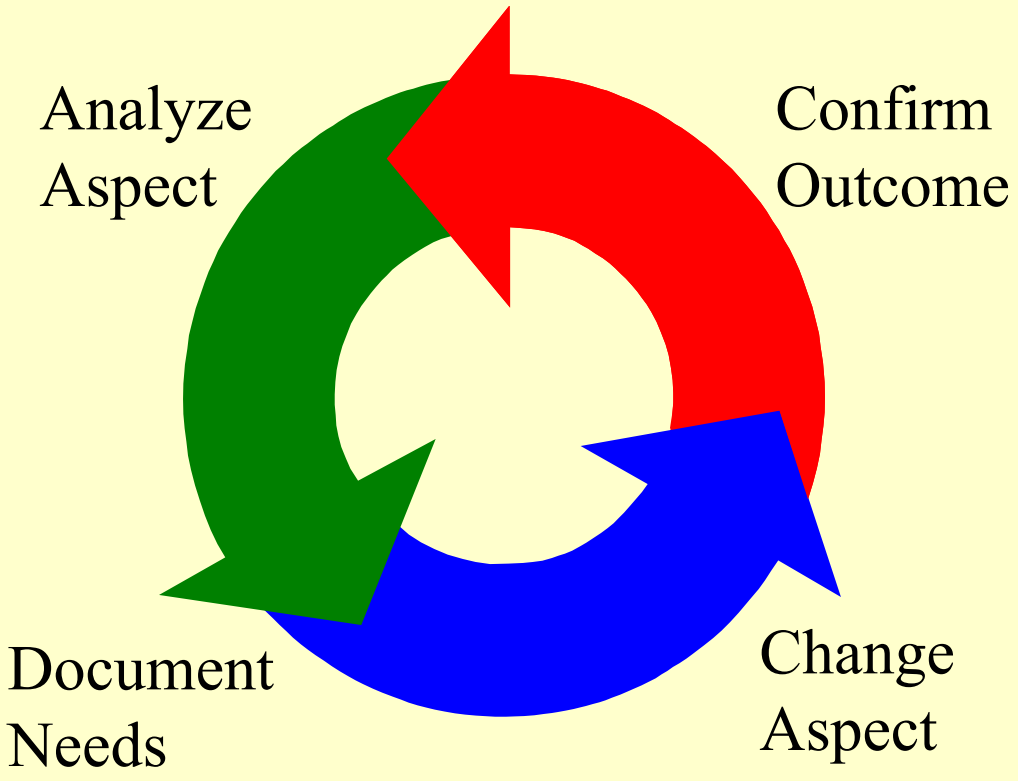
# Personnel Technical Education

- MISTI
- SANS GIAC
- CISSP Certification with $(ISC)^2$
- Summercon
- DEFCON
- Laws, rules of evidence, etc...

# Driving Security

- Privacy policy tells you what needs to be protected.
- Security policy tells you who is responsible and what is expected.
- Procedure tells you how to do it.
- Budgets and manning get it done.
- You cannot isolate security from the rest of the company; you must use their needs and input to help drive this list.
- Consolidate security oversight and responsibility, but spread the workload as wide as possible. Sell it and they will help you do it.

# Cyclical Review Process



# Cyclical Response Process

- Discovery
- Risk Assessment
- Response
- Repair
- Recovery
- Prosecution
- Modify Review Process

# Summary of Outcomes

- In three years we have:
  - Increased our application security compliance levels from 2 to 50.
  - Increased our size from 3 to 4.5
  - Updated half our 34 planned security policies.
  - Created new processes to keep us moving forward.
  - Added Intrusion Detection and improved firewalling.
  - Dealt with three legal cases based on forensic evidence.
  - Greatly increased the company awareness.

# Resources

- Wedi (HIPAA mail list)
- Stenstrom Scientific
- Red Siren
- Computer Associates
- Pentasafe
- Webwasher
- Delloitte & Touche
- Pricewaterhouse Coopers
- SANS Reading Room
- CERT
- Autotester
- HIMMS