UNIVERSITY OF Miami
SCHOOL OF MEDICINE

Security Compliance

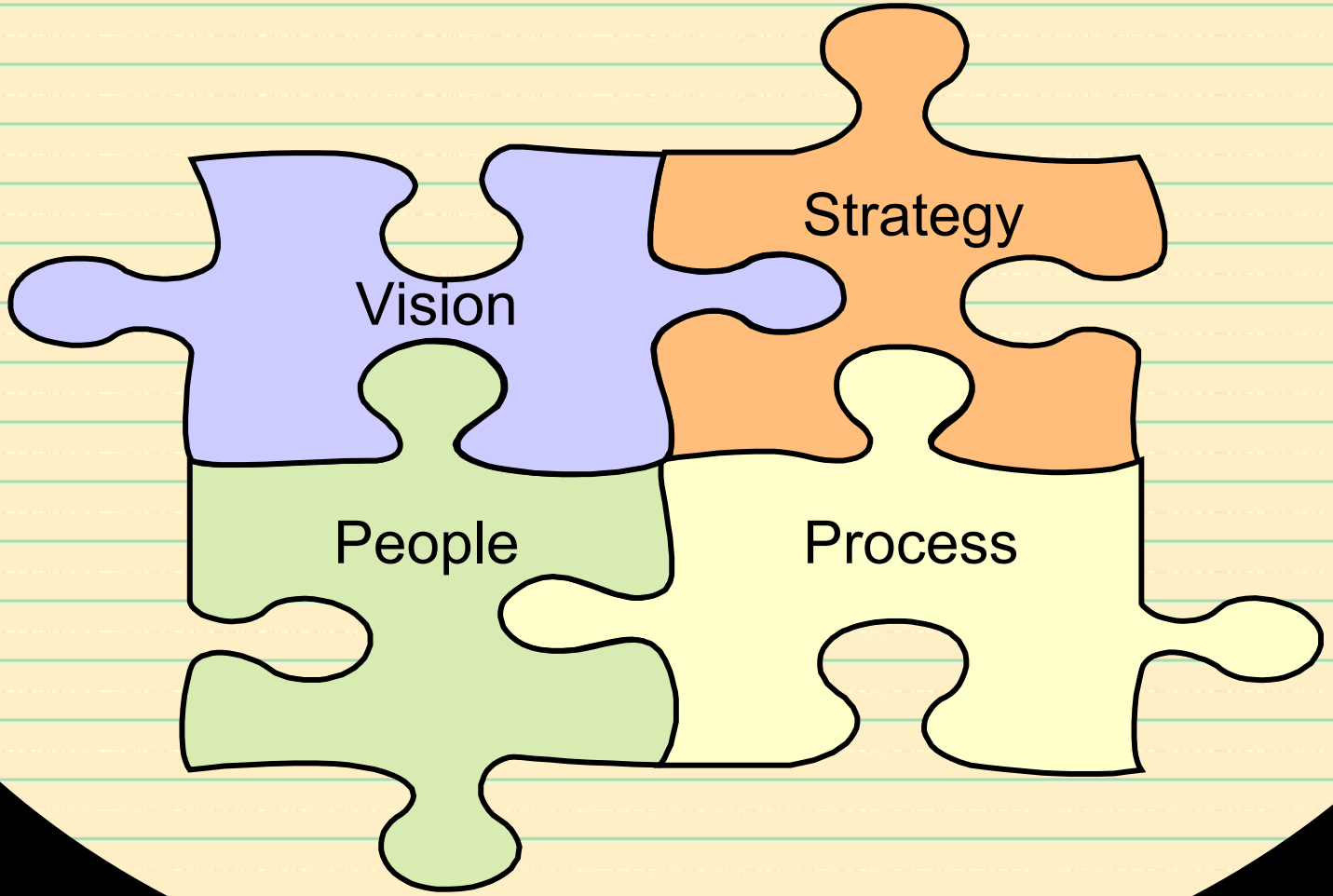
…from Planning to Practice

Sharon A. Budman

Director of HIPAA Privacy & Security

September 13, 2004

Accomplishing the Goal



Vision

- Security Compliance

  Risk Assessment is the first step towards Security Compliance

Understanding the Challenge
The Strategy – Risk Assessment

- Identification of systems, key stakeholders, and associated information related to e-phi within the organization.
- Design a strategy to inventory all systems that maintain or transmit e-phi.
- Develop and disseminate a data collection tool that details the systems, users, and information.
- Analyze the data.

The Goal of the Analysis Process

- Protect the organization and its ability to perform its mission.
  - IT assets facilitate our mission
  - The process should NOT be treated primarily as a technical function but rather as an ***essential management function of the organization.***

NIST – SP800-30 (as referenced in the security rule)

Defining the People/Players Who are they?

- Leadership Support/Sponsor
- Steering Committee -Leadership Group
- Key Stakeholders – System Owners
- Risk Assessment Team

The Structure - Hybrid

- Decentralized IT Structure
- Decentralized Clinical Departments
- Decentralized Medical Records
- Research – Outside of the Covered Entity

Planning Considerations
Types of Risk Assessments
Quantitative vs. Qualitative

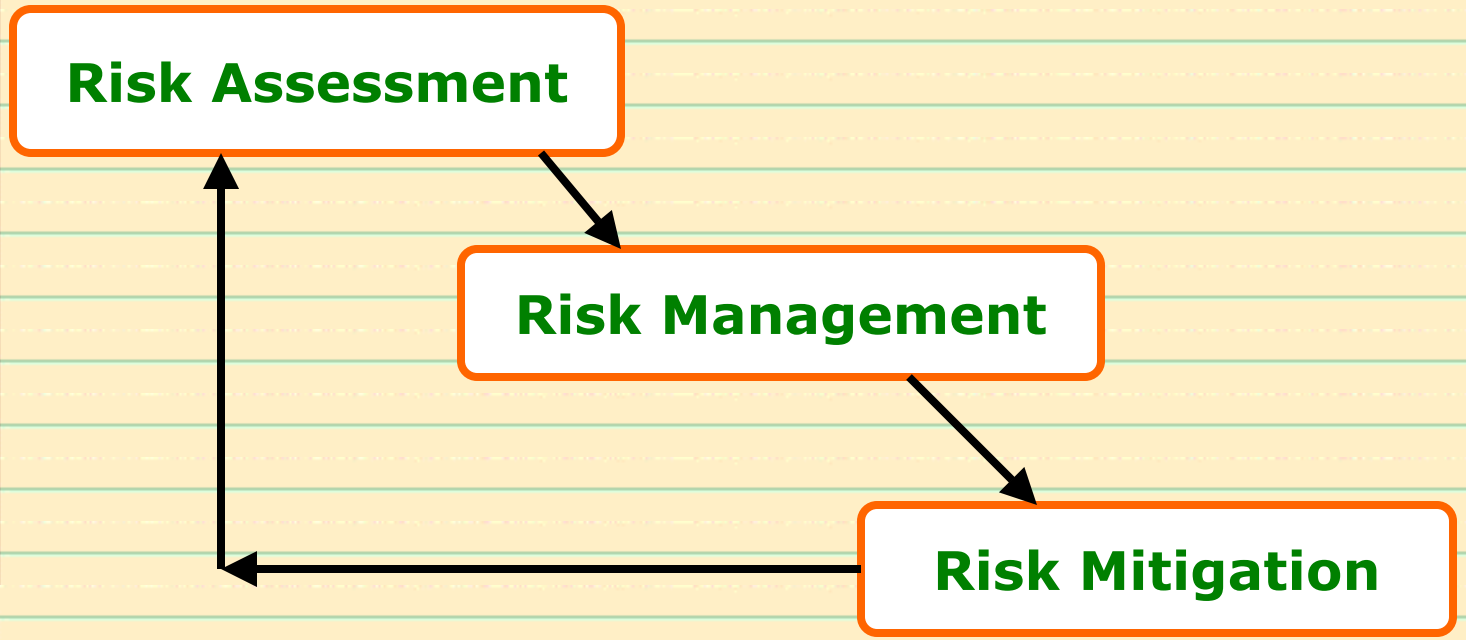
Quantitative Risk Assessment

- Main Advantage
  - Provides specific quantifiable measurements of the magnitude of the impacts which can be used in a cost benefit analysis of the recommended controls.
- Main Disadvantage
  - Values must be assigned to the assets and determining accurate values may be difficult.

Qualitative Risk Assessment

- Main Advantage
  - Prioritizes the risk and identifies the areas for immediate improvement.
- Main Disadvantage
  - Does not provide specific quantifiable measurements of the magnitude of the impacts, therefore, making a cost benefit analysis of any recommended controls difficult.

Risk Analysis
3 Phase Approach
A Continuous Process



Defining the Phases of Risk Analysis

Risk Assessment - Determine the hazards, the exposure and characterizing the risk to the organization

Risk Management – Analyze and select the policies and control alternatives based on the risk assessment findings.

Risk Mitigation – Implement the selected policies and controls and subsequently monitor their application.

Risks to Covered Entity

- Permanent loss or corruption of EPHI
- Temporary loss or unavailability of medical records
- Loss of financial cash flow
- Unauthorized access to or disclosure of EPHI
- Loss of physical assets
- Damage to reputation and public confidence
- Threats to patient safety
- Threats to employee safety

PRIORTIZATION OF RISK

….as defined by Leadership

- –Patient Care Impact
- –Financial Loss
- –Legal Implication Loss
- –Loss of Reputation

The Roll-out

- Embarked on Quantitative Risk Assessment
- Unable to readily obtain necessary values to incorporate into the analysis
- Changed gears and moved towards Qualitative Risk Assessment

Current Status

- Enlisted all key system owners for data collection purposes
- Obtained information related to systems with E-phi
- Prioritization of Systems based on Leadership Priorities
- Expanded infrastructure

Living and Learning

- Garner leadership support
- Encourage Buy-in from Key Stakeholders
- Use HIPAA for Continuous Process Improvement
- Look at HIPAA in a positive realm and use it as a catalyst to effectuate change

Questions????

Contact information:

Sharon A. Budman

sbudman@med.miami.edu

Director of HIPAA Privacy & Security

University of Miami Office of HIPAA Privacy & Security

305-243-5000

UNDERSTANDING THE KEY ELEMENTS OF RISK ANALYSIS TO MEET THE HIPAA FINAL SECURITY RULE

Caroline Hamilton, President

RiskWatch, Inc.

RISK ANALYSIS IS A MANAGEMENT TOOL – IT ELEVATES THE SECURITY FUNCTION UP TO THE BOARD ROOM

"IF YOU CAN'T MEASURE IT,

YOU CAN'T MANAGE IT!"

--Peter Drucker

5 STEPS IN THE HIPAA SECURITY RISK ANALYSIS

- Define & value all assets
- Analyze Existing Threats
- Survey personnel to discover vulnerabilities in handling protected electronic health information.
- Analyze the data.
- Write the report.

ALL SECURITY RISK ANALYSIS ELEMENTS COME FROM GOVERNMENT AND AUDIT GUIDELINES

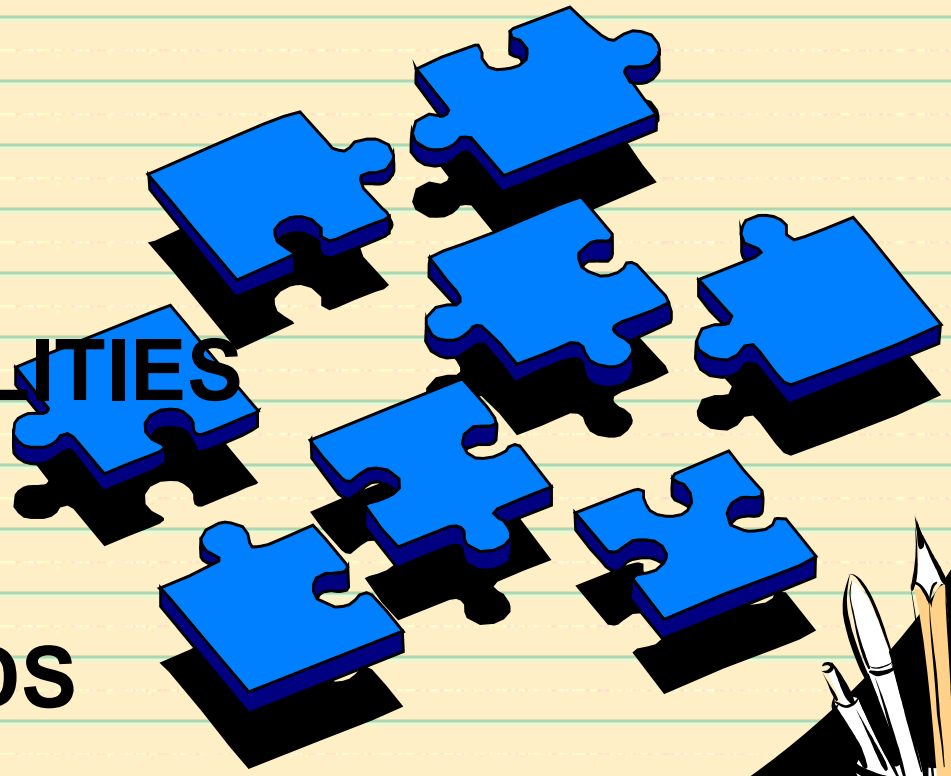
ASSETS

THREATS

VULNERABILITIES

LOSSES

SAFEGUARDS



SAMPLE ASSET CATEGORIES

- Applications
- Clinical Staff
- Communication Systems
- Data Centers
- Databases
- E-Health Info
- Electrical Power
- Facilities
- Hardware
- Medical Records
- Networks
- Monitoring Equipment
- Patients
- Personnel
- Pharmacy
- Security Systems
- Software
- System Software

THREAT INFORMATION

- ***Quantified threat data is hard to find.***
- Categories of Threats:

  Natural Disasters, Criminal Activity

  Malicious Code, Hackers, Fraud
- Includes collected data from Web Sources, government data, weather data, crime casts, global info services, access control systems, incident logs.
- You can customize with data from internally collected sources

STANDARD AND LOCAL THREAT DATA FREQUENCY ESTIMATES PER ORGANIZATION PER YEAR

Selected Threats	LAFE	SAFE
Biological Contamination	0.05	0.05
Budget Loss	0.50	0.50
Cold/Frost/Snow	5.00	5.00
Communication Loss	300.00	100.00
Competition	5.00	5.00
Data Destruction	20.00	20.00
Data Disclosure	12.00	3.00
Data Integrity Loss	30.00	3.00
Electromagnetic Interference	5.00	5.00
Errors, General/All	150.00	150.00
Fire, Catastrophic	0.01	0.01
Fire, False Alarm	2.00	2.00
Fire, Major	0.05	0.05

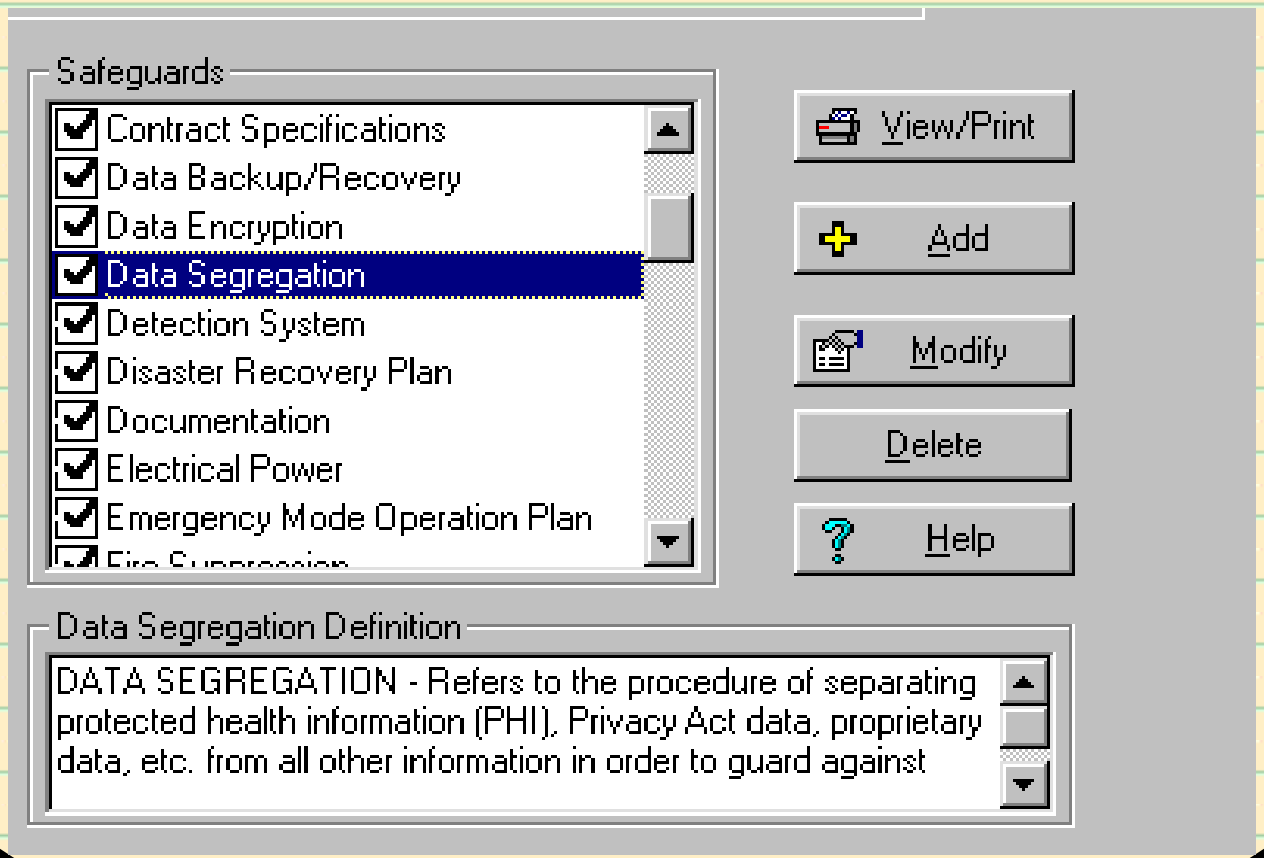
Finding Vulnerabilities Through Electronic Surveys – Finding out how people do their jobs

- Surveying the entire organization
- Using a non-threatening scientific approach
- Must include complete audit trails
- Should include different levels of the organizations

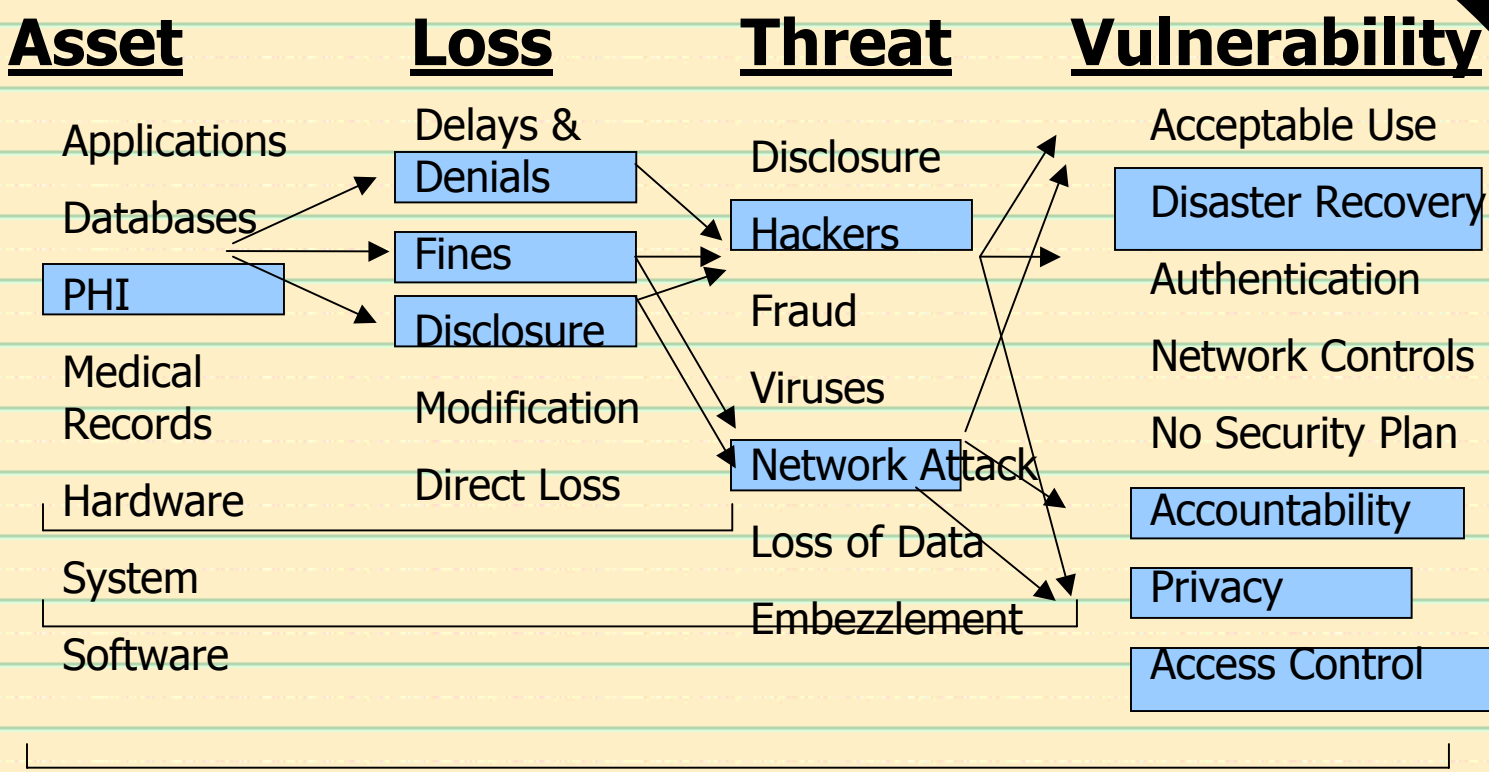
ANALYZE POTENTIAL LOSS CATEGORIES

- Delays and Denials of Service
- Disclosure of PHI
- Direct Loss (Computers Destroyed)
- Regulatory Fines (Liability)
- Modification of Data
- Reputation (Credibility)
- Direct Related (Sum of the Above)

HIPAA-REQUIRED SAFEGUARD CATEGORIES

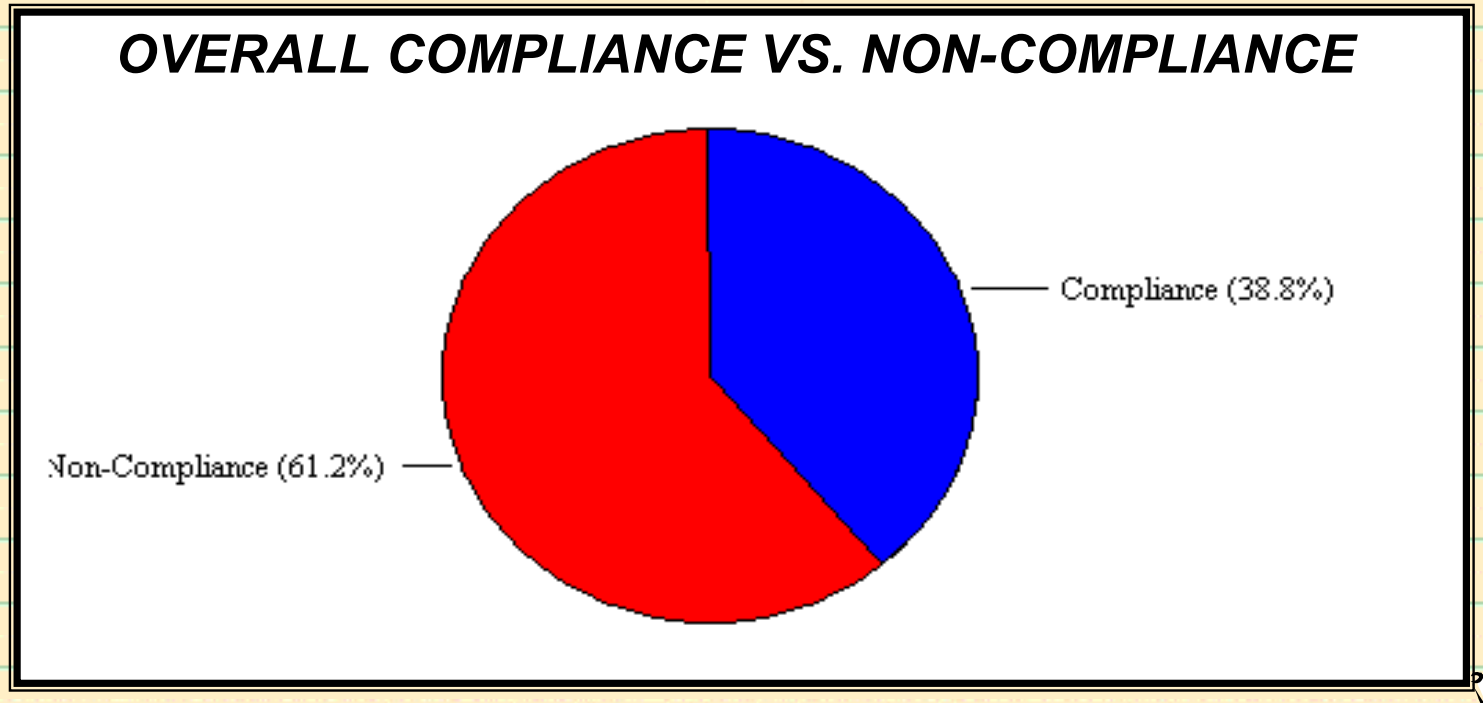


Linking Relationships

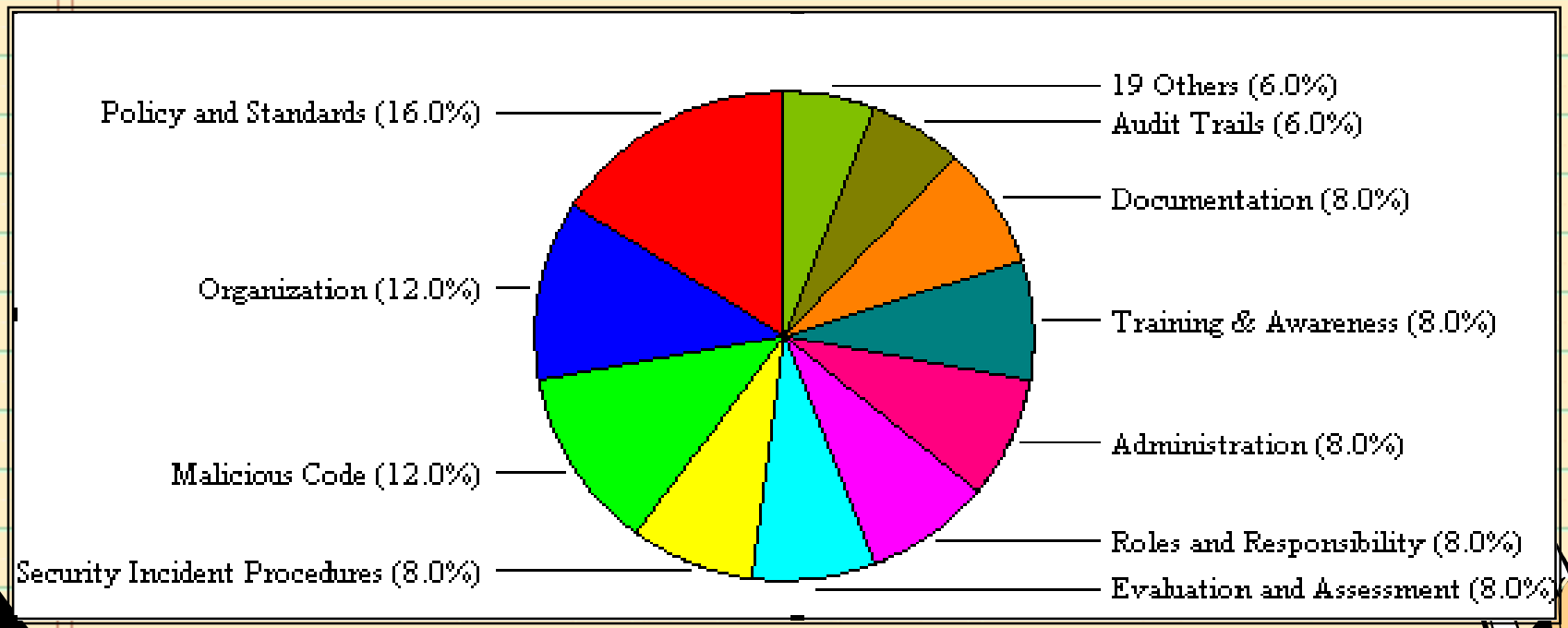


Risk = Asset * Loss * Threat * Vulnerability

HOW TO ILLUSTRATE RESULTS OF THE ANALYSIS FOR MANAGEMENT



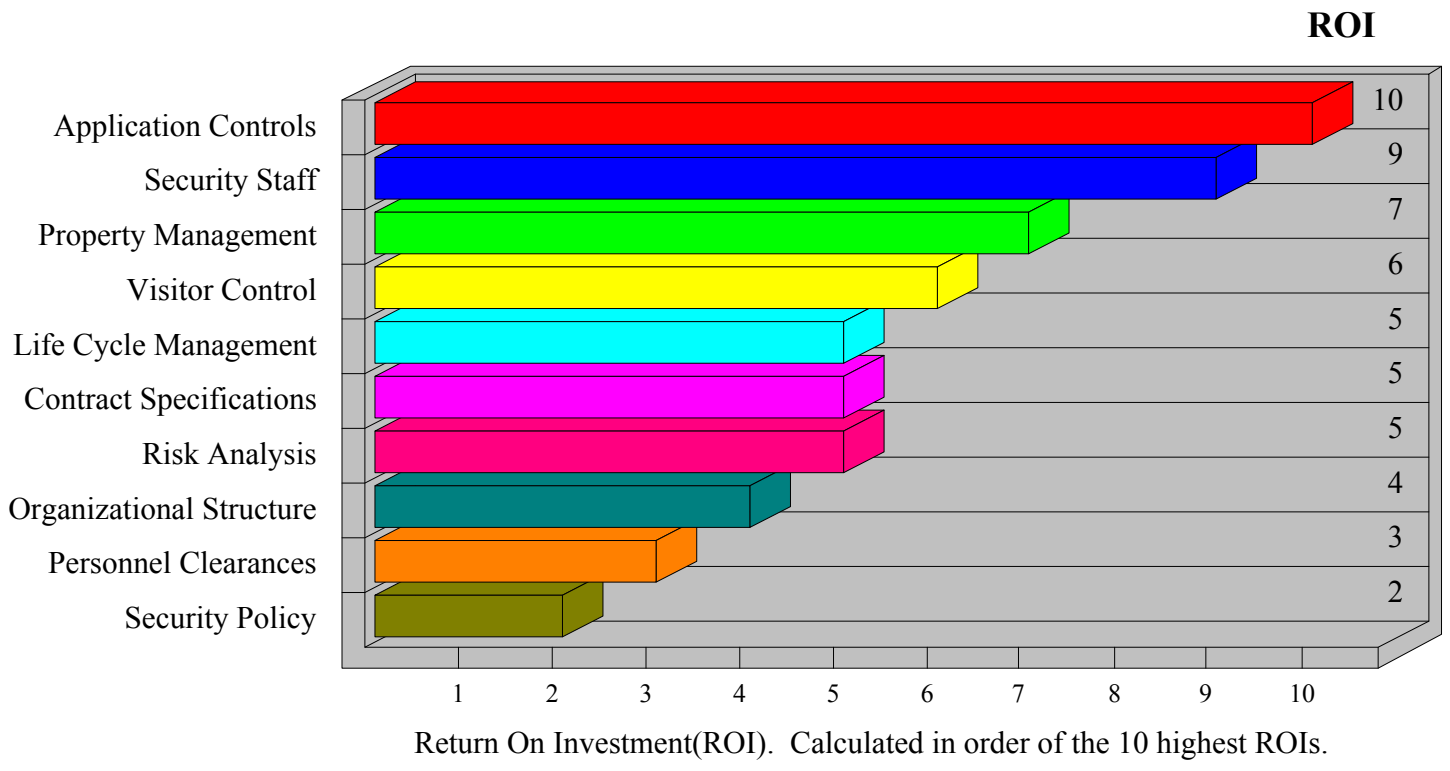
Vulnerability Distribution Report Indicates Weak Security Areas By Category and Backed up by Audit Trails



How To Calculate Return on Investment

1. Finish Disaster Recovery Plan 2000:1
2. Finish the Security Plan 1200:1
3. Distribute Security Policy 943:1
4. Mandatory Security Training 75:1

RISK ANALYSIS REPORTING
RECOMMENDED CONTROLS
BY RETURN ON INVESTMENT (ROI)



USING COLLECTED DATA TO BENCHMARK HEALTHCARE RISKS

- **By Hospital, by Systems, by Business Unit, by Region**
- **Common standards, terms and definitions**
- **Use for budgeting purposes --- determining ‘reasonable precautions’ --- ‘as good as’**

THE BOTTOM LINE

The Risk Analysis Process means Ongoing Compliance Measurement and Validation

- **Data Security/Privacy regulations in Healthcare will continue to increase.**
- **The Risk Analysis is a key to demonstrating on-going HIPAA compliance**
- **Properly done, a risk analysis will credibly measure HIPAA compliance, identify vulnerabilities, justify capital improvements and focus & prioritize the security budget.**

chamilton@riskwatch.com

www.riskwatch.com