

Getting Started with Your HIPAA Security Self- Assessment and Planning

*Presented to the HIPAA Summit VII
Baltimore, MD
September 15, 2003*

John Piazza



Holt Anderson



Presentation Segments

- Introduction to Gap and Risk Analysis: Holt Anderson
 - Regulation overview
 - Gap analysis, risk assessment
 - Automating the process - tools
- Real World Compliance John Piazza
 - Univ. of Alabama - Birmingham
- Q&A



HIPAA Enforcement

- **Office of Civil Rights (Privacy)**
- **CMS (Transactions, Code Sets, Identifiers, Security)**
- Justice Department
- FBI
- Lessons learned from fraud & abuse
- Accreditation reviews
- Plaintiff's bar & courts
- Business Continuity

HIPAA Enforcement at CMS

New office established in CMS:

- » Establish and operate enforcement processes
- » Develop regulations
- » Obtaining voluntary compliance through technical assistance
- » Process will be complaint driven

Impact of Not Complying

- Possible litigation
- Loss of public confidence
- Penalties
 - Civil monetary for violations of each standard
 - Criminal for wrongful disclosure of protected health information
 - No private right of action



Business Risks in Security

- Loose security implementation may open the door to litigation for privacy violations
- Scope and complexity of current environment with frequent technology changes
- Unquestioning reliance on vendors and “HIPAA Compliant” solutions
- Covered entity has not done thorough analysis and compliance effort and is found negligent

Beginning the Process

- Determine scope of project
- Obtain top management approval
- Engage key players from each affected area
- Build assessment team
- Train assessment team to “standard” of assessment
- Do the assessments

Gap Analysis

- What is your current state?
- What do the regulations say?
 - Required Standards
 - Addressable Standards
- Where is the mismatch (gap)?
- What is reasonable and appropriate to do within a tolerable risk?

Planning for Your Gap Analysis

- Determine the scope of the analysis
 - Which organizations, divisions, departments, affiliated entities, etc.?
 - What level of management will participate?
 - What level of detail will be collected / expected?
- Utilize information already in hand
 - Inventories of hardware and applications
 - Gather and catalog policies and procedures from across the organization

Issues with Larger Organizations

- More complex organizations require more detailed planning and consistent execution of the analysis.
- The key to a good outcome is gathering information consistently across the enterprise.
- Make assignments consistent with the responsibilities of each subdivision
- Get your “team” on the same page – training before the information gathering process begins – set consensus expectations

During & After Information Gathering

- Develop management reports
 - Key areas of concern
 - Trends
- Construct alternative paths to compliance
 - Business impacts / risks
 - Clinical impacts of alternatives
- Formalize risk assessment
- Make choices and proceed with an implementation plan leading to compliance

Risk Assessment

- § 164.308 Administrative Safeguards
 - Implementation specifications
 - (A) **Risk Analysis** (Required) Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information by the covered entity.
 - (B) **Risk Management** (Required) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)

About NCHICA

- 501(c)(3) nonprofit research & education
- Established in 1994
- ~275 organization members including:
 - Providers
 - Health Plans
 - Clearinghouses
 - State & Federal Government Agencies
 - Professional Associations and Societies
 - Research Organizations
 - Vendors
- Mission: Implement information technology and secure communications in healthcare

NCHICA's HIPAA Efforts

- Task Force and 5 Work Groups
 - (450+ individuals participating from members)
- Developed documents, training, and tools
- Gap analysis tools designed to provide an early cut at self-assessment
- Education has been pleasant by-product
- Consultants use tools to provide consistency and thoroughness in approach for smaller organizations



- About NCHICA
- HIPAA Resources**
- Membership
- Yellow Pages

What's New

- 2003 Annual Conference & Exhibition:**
- [agenda](#)
 - [sessions](#)
 - [credits](#)
 - [speakers](#)
 - [sponsors](#)
 - [exhibitors](#)
 - [hotels](#)
 - [golf](#)

- Register now!**
- [members](#)
 - [non-members](#)

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA)

- organizations dedicated to improving healthcare through information technology and secure communications.
- hospitals and health plans
 - medical and dental practices
 - professional societies
 - national, state and local government agencies
 - law firms
 - healthcare and pharmaceutical associations
 - health education and research organizations

NCHICA is a good example of how the many sectors of the healthcare industry can work together to make a difference. NCHICA activities include:

- [HIPAA Task Force](#)
- [North Carolina Emergency Department Database](#)
- [Provider Access to Immunization Records Securely \(PAIRS\) Project](#)

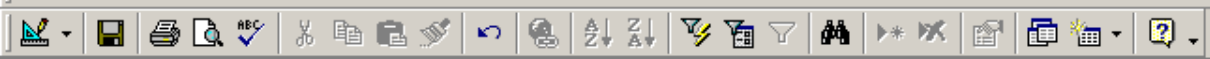
- HIPAA EarlyView™ Tools
- Sample Documents (Reviewed)
- Sample Documents (Not Reviewed)
- Regulations
- Speakers Bureau
- HIPAA Calendar
- HIPAA Task Force
- Presentations
- Links

Goals of EarlyView Tools

- Closed-end gap questions true to the regulation
 - No “extra” questions
 - No room for “Maybe” – only “Yes” “No” or “N/A”
- “Things to think about” provided to expand considerations of how one might approach a particular standard
 - Potential alternatives to compliance
- Create a thorough understanding of the rule and the impact on the organization
 - Management reports highlight action items and document due diligence

The Tools' Structure


- Built around the assessment process
- Questions keyed to the regulation standards
- Space for free-text documentation of due diligence
- Presented in same order as regulation
- Links to the regulation text
- Documentation of progress available for management purposes
- Can be updated and new management reports printed as compliance progresses



Main Menu

HIPAA EarlyView™ Security Version 2.0

Your Dept or Role: **Change**

- Coordinator Functions
- Edit Departmental Information
- Glossary of Terms
-  **Security Self Assessment**
- Browse the Security Regula
- Choose Report to View or P

Copyright© 2000-2003 NCHICA www.nchica.org

Security Self Assessment

HIPAA Security Self Assessment

Section: Policies and procedures and documentation requirements ?

Standard: Documentation ?

Implementation Spec.: Updates ?

165. Does your policy specify a periodic review and revision of your security policies and procedures?

Answer:

Comments: Our policies specifies that we review at least annually or anytime there is a major change in the organization.

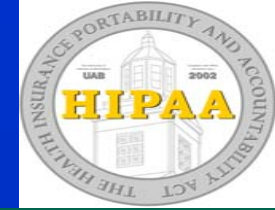
Copyright© 2000-2003 NCHICA www.nchica.org All Rights Reserved

Record: 165 of 165

Begin Here

John Piazza

About UAB - HIPAA



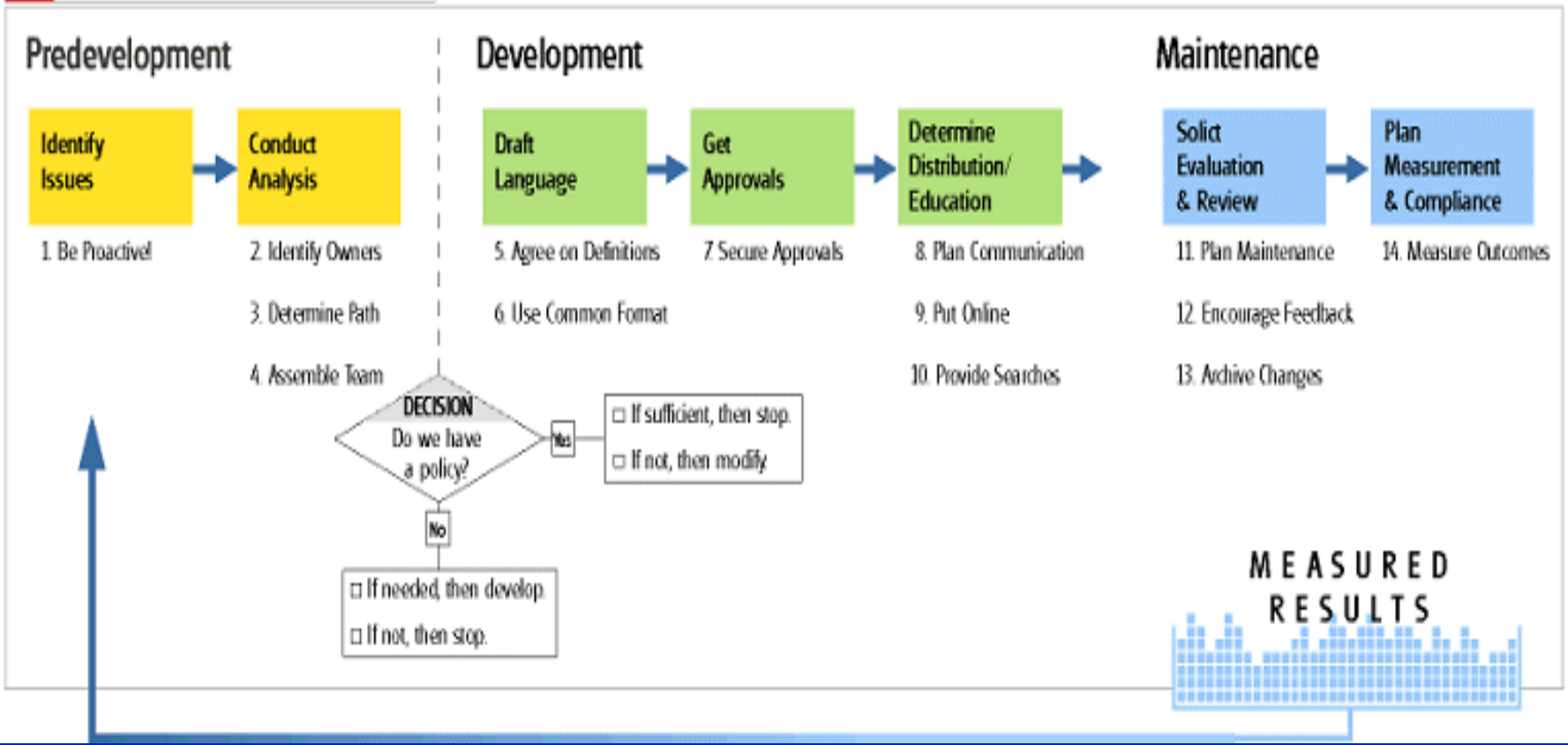
- Over 200 Departments
- Over 100 Centers
- 7 major hospitals
- 6 satellite/offsite Clinics
- 87 square blocks
- 1.3 billion budget
- 400 mil research
- 13 schools
 - 6 covered by HIPAA
 - 7 by GLB
 - 50k+ patients annual
- 12,000 employees under HIPAA – 5000 under GLB/FERPA
 - 6000+ in health care research/support
 - 6000+ in direct health care delivery/support
- graduate/professional
- 30,000 nodes
- Windows
- Mac
- Unix
- Novell
- Linux
- IBM 370's /400's
- You name it...

Policy Development Process

Policy Development Process (ACUPA)

POLICY DEVELOPMENT PROCESS WITH BEST PRACTICES

! BEFORE you start...
Get authorization and support for the process.



Developing Policies and Procedures

- Mission
- Goals
- Objectives
- Policy-shalls
- Procedures - shoulds
- Guidelines – considerations/options/
recommendations
- Checklists – specific “how to”

Ranked Credible Policy Sources

- 1 - Law (statutory-admin- and case)
 - HIPAA / GLB / FERPA / OS – Eli Lilly v FTC
- 2 - Standards setting organizations
 - ISO / NIST / ANSI
- 3 - Industry best practices Groups
 - NCHICA / WISCONSIN
- 4 - Trade Associations/Groups
 - CERT / SANS / ISSA
- 5 - Experts/articles(white papers)
- 6 - In house “experts”/processes☺(found in many nooks and crannies)

Policies

- A statement that reflects the philosophies, attitudes, or values of an organization related to a specific issue.
- A paragraph or perhaps two – but not pages.
- Might say “what” but not “how.”
- Procedures, standards, guidelines, checklists, forms, all must implement, reflect, and support the applicable policy or policies.
- The entire set of statements is sometimes considered to be the “Policy.”

Policy example

- **Security Management Process:**

- **POLICY STATEMENT**

It is the policy of The University of Alabama at Birmingham to employ a formal security management process for the protection of data and related technology, utilizing appropriate analysis and management techniques to mitigate risk in preventing, detecting, containing, and correcting threats, vulnerabilities, and exposures. This process is reinforced through routine systems activity reviews and evaluations and may involve sanctions.

Policy Formulation -- Formal

- Standard format adopted by the organization and applicable to single issues, even within a particular topic area (e.g., technology):
 - Policy identifier (title, number)
 - Effective or draft date
 - Rationale statement
 - Policy statement
 - Definitions
 - Procedures/guidelines/standards
 - References (including other applicable policies)
 - Responsible office
 - Review schedule

Policy Formulation -- Informal

- In the same document, narrative paragraphs on each issue area outlining the University's attitude/position in that area.

Standards

- A statement dictating the state of affairs or action in a particular circumstance.
- A rule established by a recognized authority, with no deviation allowed.

Standards -- examples

1. Each school/department and center shall assess the relevant losses due to risk exposure
2. Each school/department and center shall prioritize the risks and vulnerabilities that have been identified as part of the risk analysis
3. Each school/department and center shall conduct risk analysis that addressed both intentional and unintentional risks

Procedures

- One or more sentences describing how to accomplish a task or reach a goal – directive statements.
- The specified actions are generally mandatory for the specific situation.
- More explanatory text involved.
- Sequence not necessary but sometimes is important.

Procedure example

Security Management Process

1. *Each school/department and center should develop a plan for managing identified risks (V₁ 127)*
2. *Each school/department and center should have a written virus protection policy (V₁ 263)*
3. *Each school/department and center should have procedures for virus identification and containment (V₁ 264)*
4. *Each school/department and center should use a virus scanning software on all computer systems (V₁ 265)*
5. *Each school/department and center should document the procedures for updating anti-virus software periodically (V₁ 266)*

Procedures – other examples

- Contact the RUST Network Center at 205-934-0001 to activate a data jack.
- Contact the ITS Customer Services if you've forgotten your password.

Guidelines

- Provides ideas/things to consider for fine tuning a local process
- Information about how to accomplish some task or reach a specific goal.
- Suggestions; not mandatory, but a good idea.
- An element of “best practice” -- alternate actions might be available and might work, but what is being provided have proven to be the fastest, cheapest, etc.
- More explanatory text involved.
- May demonstrate an “ideal’ flow of the policy in action.

Guidelines -- example

- When possible install the software from the CD, as technicians have had trouble accessing the web site at times.

Checklists

- One or more statements dictating how to accomplish a task – “commands”.
- Applicable to an immediate circumstance, and mandatory in that situation.
- Immediately at hand.
- Simple language.
- No amplifying text.
- Sequence is always important.
- Flowcharts.

Checklist example.

Screenlock/Password activation in Windows

Using your mouse cursor:

1. Click on the “start” button on your screen
2. Click on ‘settings’ then ‘control panel’ then ‘display’
3. Next - Click on ‘ screen saver’ in the ‘display properties’ window
4. Select a ‘screen saver’ in the drop down menu on left central side of the ‘display window’
5. Check the box below the screen saver window labeled ‘password protected’
6. To the right of the password protected checked box click on the ‘wait____minutes’ box and click the up or down arrow until you reach five minutes
7. Click on ‘apply’ in the lower right corner then ‘okay’ in the lower left corner and you are now screensaver /password(screenlocked) protected requiring your password each time the machine is left unattended for five minutes or more.

Security Management Process

- Process to prevent, detect, contain, and correct threats, vulnerabilities and exposures
 - Risk Analysis
 - Risk Management
 - Sanction Policy
 - Information System Activity Review

Definitions

Process that includes risk assessment/analysis/budgeting/prioritization/implementation of appropriate countermeasures

RISK

Potential for harm or loss

RISK MANAGEMENT

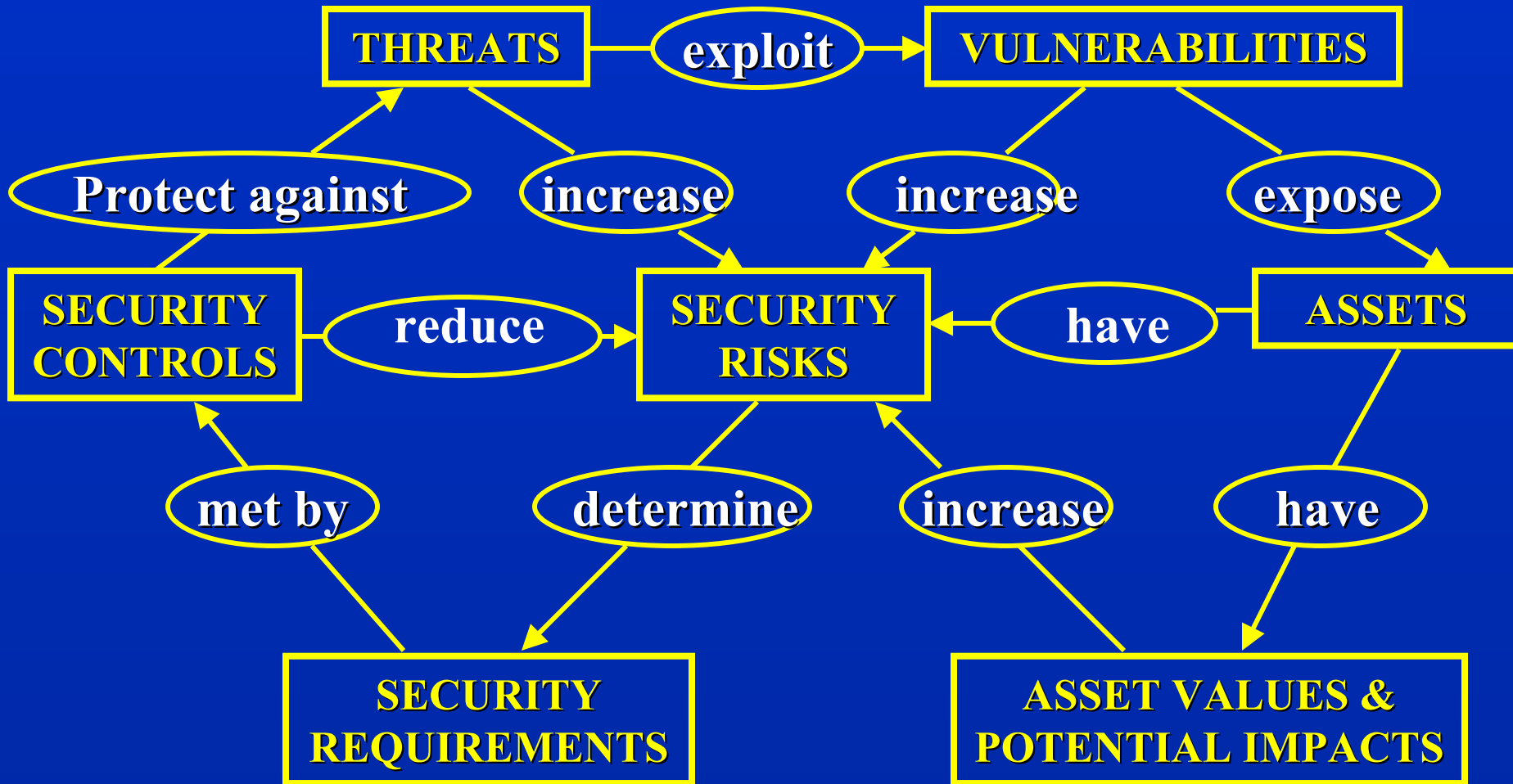
RISK ANALYSIS

Analyzing an environment and the relationships of its risk related attributes

RISK ASSESSMENT

Assignment of values to assets, threat frequencies, consequences etc

Risk Components Relationship



Benefits of Risk Assessment

- Some of the specific benefits include:
 - Understand *what is at risk*
 - The *value at risk* – i.e. information assets and with confidentiality, integrity and availability of assets
 - *Kinds of threats* and their financial consequences
 - *Mitigation analysis*: what can be done to reduce risk to an acceptable level

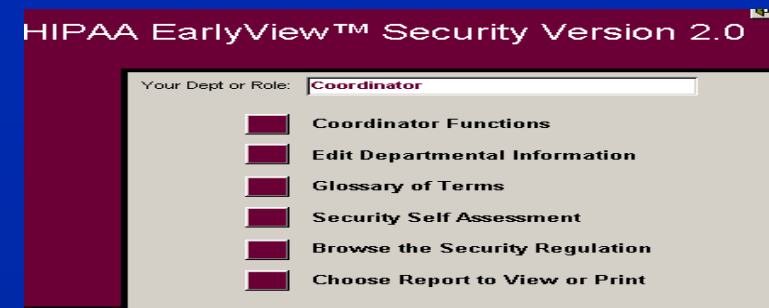
Two types of Risk Assessment

- Quantitative – dollar values/metrics/ real numbers
 - Easy to automate
 - More complex/accurate/tedious
 - Cost benefit analysis provided
 - Independent objective methods
 - clear
- Qualitative – ranking - high med low
 - Allows for owners/users/expert input as to value
 - Faster/easier once all are trained in the process
 - Less accurate

Types of Risk Assessment (2)

- Non-Automated Assessment
 - Live training 3 people/3 days/dept
 - Manual actuarial guess analysis
 - ~18 months- 3 yrs
 - i.e. OCTAVE, COBRA
- Automated Assessment
 - Automated questionnaire for each department
 - Standardized actuarial analysis
 - ~6 months
 - E.g. HIPAAWatch, Buddy System

Use of Automated Tools – Integrate the best of each (1)



- Quantitative risk analysis software
- Automated method of determining what controls are needed to protect organizations' assets
- Server based
- Automatic actuarial computations
- Customizable
- Countermeasure recs
- Reports/resources-legal



Self-assessment / Gap Analysis Tools

HIPAA EarlyView™ Security

HIPAA EarlyView™ Privacy

Integrate Automated tools

| | |
|-------------------------------|--|
| Workforce Clearance Procedure | If you choose not to implement this addressable implementation specification, have you performed a risk and cost analysis and documented your decision? |
| Termination Procedures | Does your organization have documented policies and procedures for denying physical access to terminated workforce members? |
| Termination Procedures | |
| Termination Procedures | Does your organization have documented policies and procedures for denying electronic access to terminated workforce members? |
| Termination Procedures | Does your organization have documented policies and procedures that require individuals who are terminated to surrender any electronic protected health information in their possession before he/she departs? |
| Termination Procedures | If you choose not to implement this addressable implementation specification, have you performed a risk and cost analysis and documented your decision? |

Summary of Department Answers by Regulation Standard

Standard: Access Control

| Department | Total Assigned | Yes | No | N/A | Unanswered |
|---------------------------|----------------|----------|----------|----------|------------|
| Coordinator | 7 | 0 | 0 | 0 | 7 |
| Total for Standard | 7 | 0 | 0 | 0 | 7 |

Standard: Assigned Security Responsibility

| Department | Total Assigned | Yes | No | N/A | Unanswered |
|---------------------------|----------------|----------|----------|----------|------------|
| Coordinator | 4 | 0 | 0 | 0 | 4 |
| Total for Standard | 4 | 0 | 0 | 0 | 4 |

Standard: Audit Controls

| Department | Total Assigned | Yes | No | N/A | Unanswered |
|---------------------------|----------------|----------|----------|----------|------------|
| Coordinator | 3 | 0 | 0 | 0 | 3 |
| Total for Standard | 3 | 0 | 0 | 0 | 3 |

Standard: Business Associate Contracts and Other Arrangements

| Department | Total Assigned | Yes | No | N/A | Unanswered |
|---------------------------|----------------|----------|----------|----------|------------|
| Coordinator | 7 | 0 | 0 | 0 | 7 |
| Total for Standard | 7 | 0 | 0 | 0 | 7 |

Standard: Business Associate Contracts or Other Arrangements

| Department | Total Assigned | Yes | No | N/A | Unanswered |
|-------------|----------------|-----|----|-----|------------|
| Coordinator | 2 | 0 | 0 | 0 | 2 |

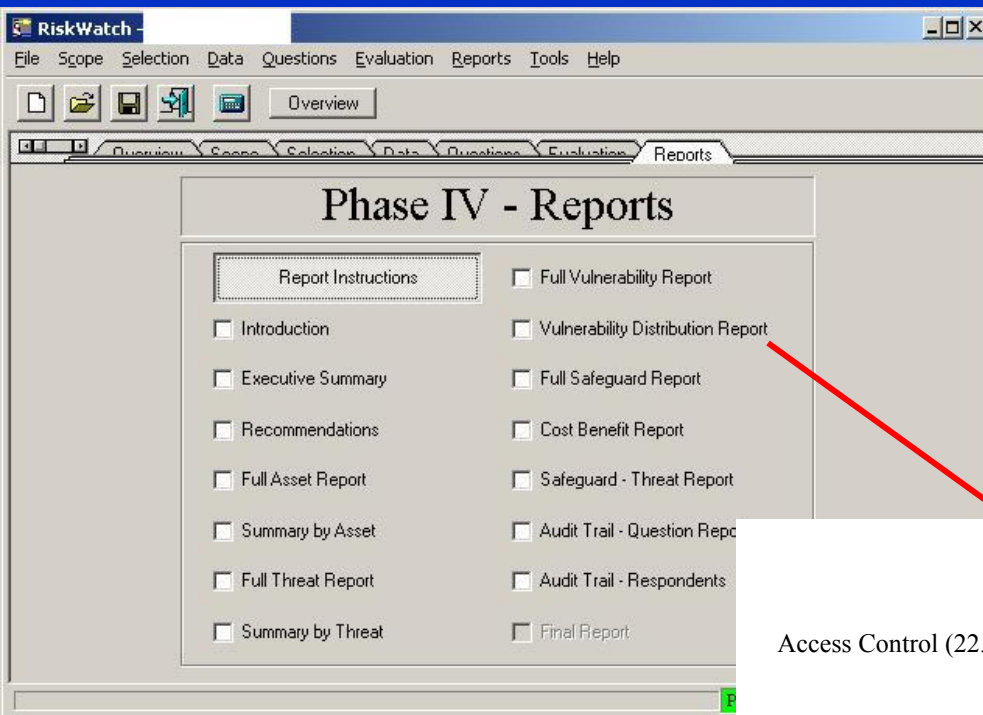
Use of Automated Tools (2)

- Gap Analysis – where are we and where do we need/want to be?
- Risk analysis – what threats exist requiring what level of protection
- Asset analysis – specific ranking of asset value
- Evaluation – maintenance piece
- Automated report generation for all levels and purposes
- Inexpensive

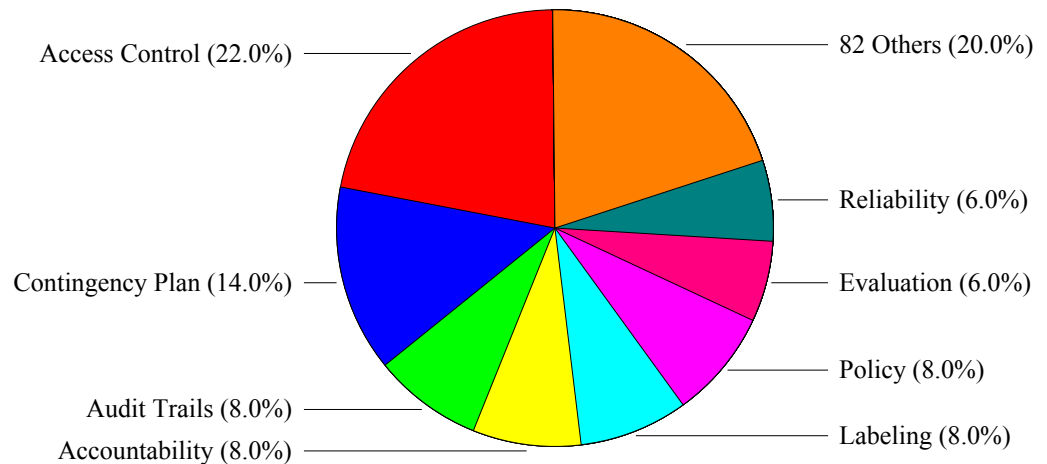
Automated Process

- At DSO, collect system/departmental information
- HIPAAWatch automatically generates questionnaire
- End user answers the questions on a web-based form
- HIPAAWatch uses this input to provide the threats they are facing, the impact of safeguards they currently have, the ROI of the safeguards, and documents the whole process (as required by the law)

Automated Process



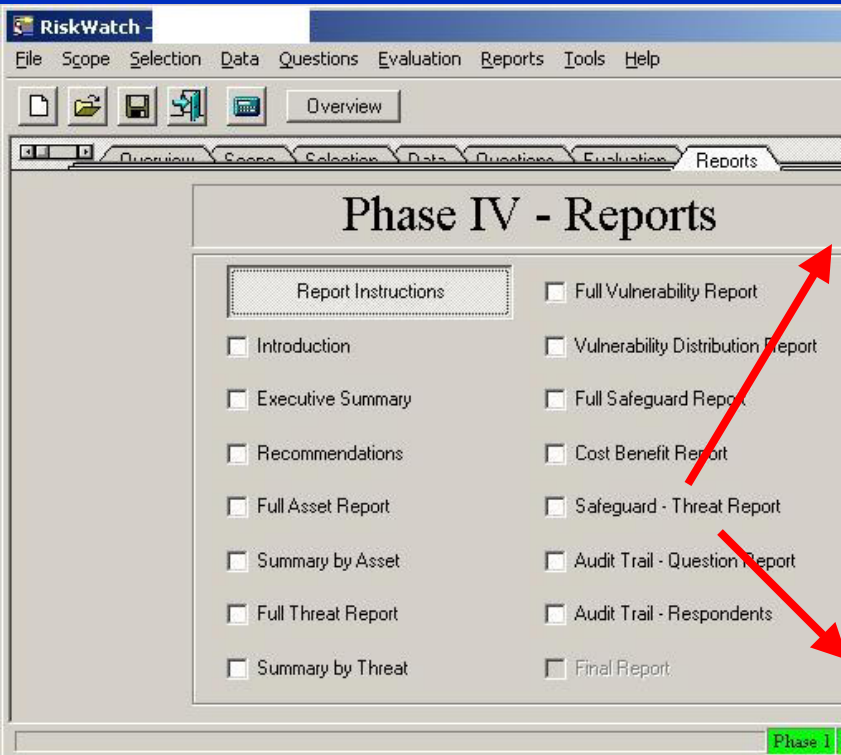
Vulnerability Distribution Report



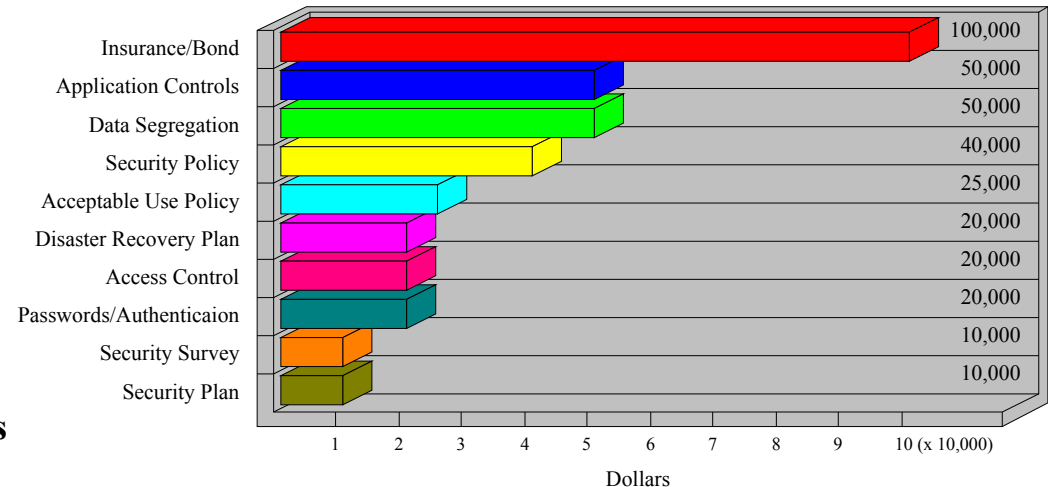
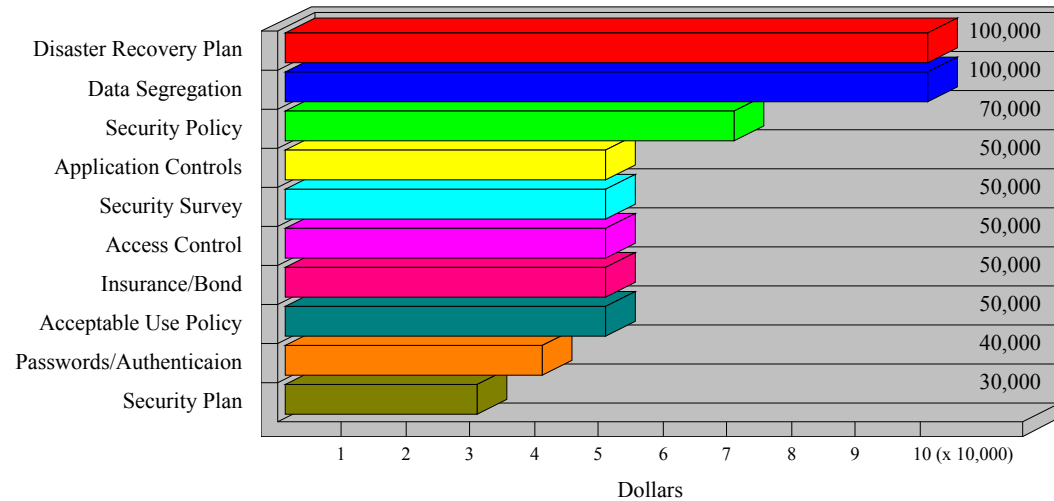
•Phase IV: Reports

Automated Process

- Phase IV: Reports

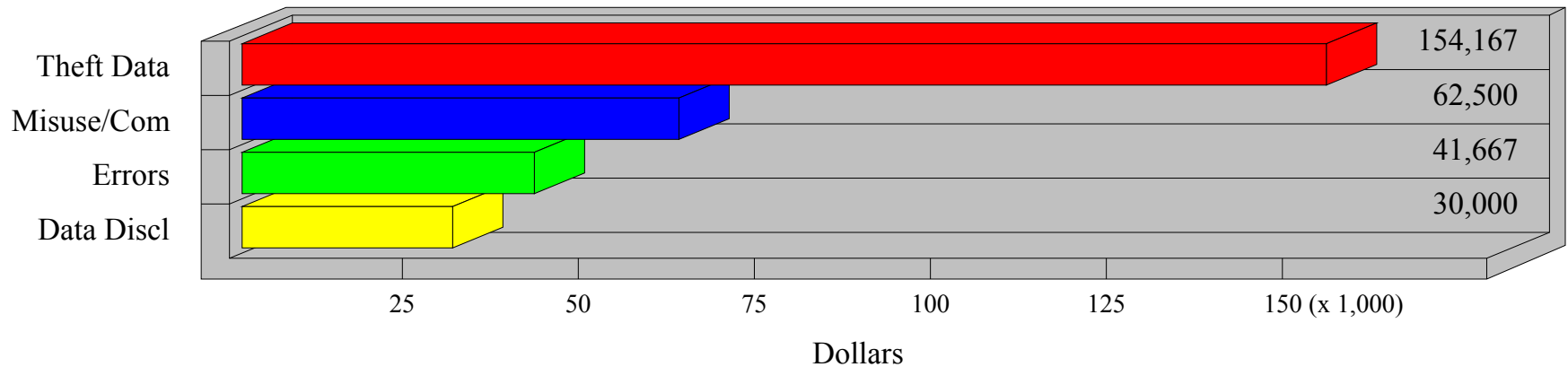


Implementation Costs



Automated Process

Annual Loss Expectancy



Fine Tuning Automation

- Use customizable software
 - Technology/software/countermeasures will change
 - Law will change
 - Actuarial data will change
 - Standards/practices will change
- Have a credible source of best practices(law/standards based organizations/NCHICA)
- Understanding appropriate fit of countermeasures for customized practices

Using Management Reports

- Advising upper management
- Getting management support
- System admin buy in
- User buy in
- Create metrics
- Justify ROI
- Create support

Sample Automated Reports

- NCHICA – approx 20+ reports & forms, such as
 - Answers by department
 - Count of answer by regulation standard
 - Questions answered/not answered by dept
 - Executive questions with model ‘considerations/answers’
- RiskWatch/HIPAAWatch – 15 reports, such as:
 - Vulnerability
 - Cost benefit
 - Full asset report
 - Full threat report
 - Countermeasures report

Crafting a Compliance Plan

- Assess need
 - Scope/depth/quality/resources
- Determine credible source material
 - Determine requirements/maintain high quality/integrity –
 - keep your fingerprints off of your source material
 - Saves time and legal fees in the long run
- Define audience/design implementation
- Recruit/reinforce senior level support using metrics/reports
- Recruit local “go to persons(experts)” in each significant area to assist in implementation
 - Assess gaps – begin security management process
- Set timetables/deadlines
- Follow established maintenance standard practice/levels
- Follow-up/fine tune/adjust

Dealing with the Skeptical

- People are sensitive to security needs
- Educate/use metrics when possible - do not surprise or scare
- Critical that you develop expertise on the law/standard practices
- Confidentiality > Good Privacy is not possible without good security!
- Security must strive for seamlessness to increase acceptance and effectiveness
- Most security implementation will happen away from the end user – don't wear out your users

Do you need a training program?

- Only if you have users - but
 - Not if they know what to do.
 - Not if it never changes
 - Not if you mind breaking the law

If users don't know what they need to know, where will they learn it?

Education and Training

- Live
- Web based
 - Database – authentication - is automated
 - Testing modules recorded in db
 - Convenient
 - Consistent
 - Cost effective
 - electronic
- New employees as part of their orientation
- All other employees/vendors/contractors to educate in new practices

Updating and Maintaining Compliance

- Minimums
 - New processes
 - Changes in
 - Workflows
 - Responsibilities
 - Laws
 - Standards/practices
 - Technology – hard and soft
 - Every three years as a minimum under HIPAA
 - Constant process for most



www.nchica.org

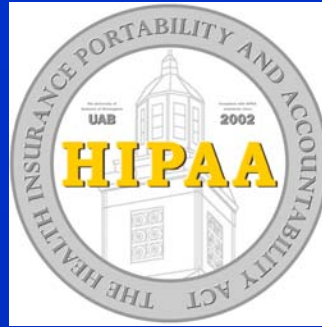
Holt Anderson, Executive Director

holt@nchica.org

P.O. Box 13048, Research Triangle Park, NC 27709-3048

Voice: 919.558.9258 or 800.241.4486

Fax: 919.558.2198



www.hrm.uab.edu/hipaa

Thank you!

John Piazza

Data Security Officer (Director) / HIPAA Compliance Officer University of
Alabama at Birmingham

[**jpiazza@uab.edu**](mailto:jpiazza@uab.edu)

UAB

AB 720

1530 3rd Avenue South

Birmingham, AL 35294-0107