HIPAA Security Compliance:

The critical role of Risk Analysis and Risk Management

April 22, 2002

Tom Grove, Director
Phoenix Health Systems

PHOENIX HEALTH SYSTEMS
healthcare IT solutions

Today's Presentation

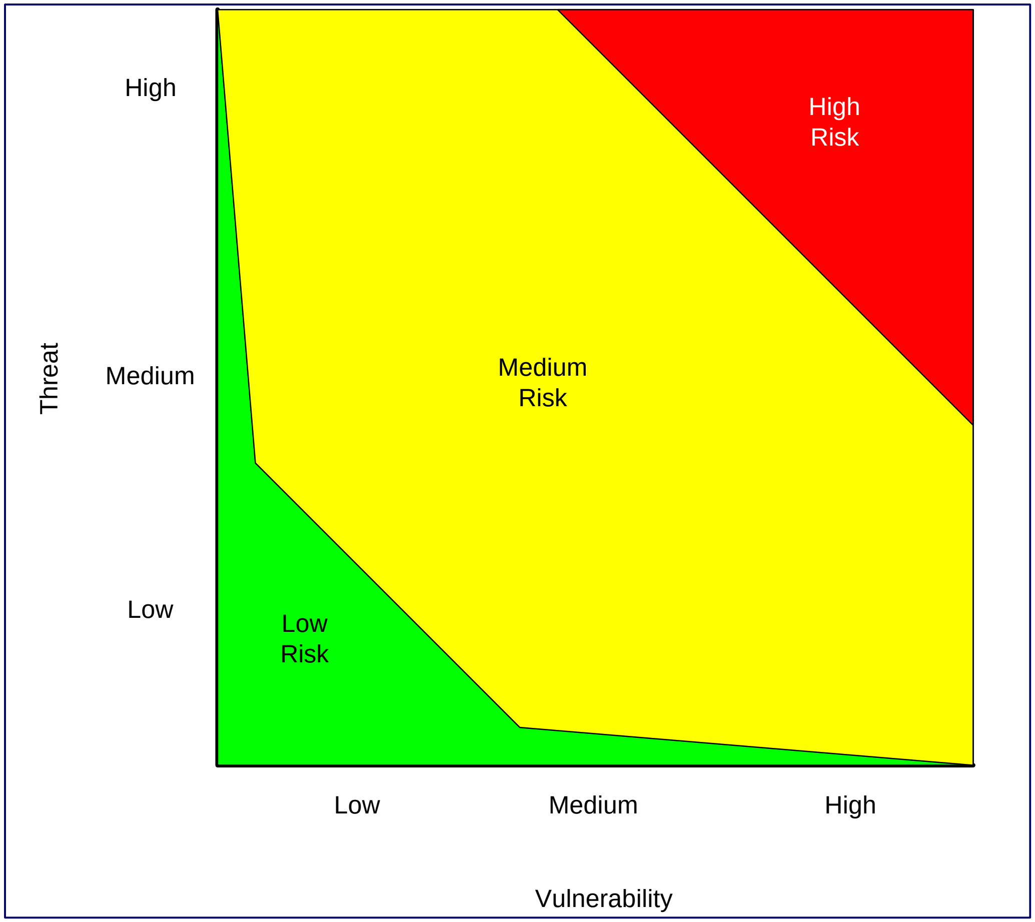
- Introduction to Risk
- Understanding Risk
- Assessing Risk
- Using Risk to Make Decisions
- Building the Risk Management Process

An Introduction to Risk

What is Risk?

- Risk is the possible loss of something of value
- Risk is a combination of a vulnerability and a threat
  - How likely?
  - How bad?
- Risks can be quantified, ranked, assessed, mitigated, and used as opportunities

The Risk Equation



Risk vs. Problem

- If the event is a certainty, you don't have a risk, you have a problem
- This includes the problems of non-compliance. For example:
  - HIPAA Security demands unique user identification. Group accounts are not a risk, they are a problem.

Risk Assessment

- The purpose of a risk assessment is to identify potential areas of loss
- Loss is usually measured as monetary, but is often indirect, such as loss of reputation
- A risk assessment provides the basis for security spending decisions

Risk Management

- Risk management is a formal process
  - Ongoing
- Risk management uses the identified risks as key drivers of the decision making process to mitigate the risks

Why do we care?

- HIPAA says we need to care
- Risk management is how to balance risks with resources to justify appropriate security decisions
- Well thought out risk decisions are the best defense against claims that your decisions don’t meet the rules

Cautions about measuring risk

- Project risk vs. Security risk
  - HIPAA requires a risk assessment of security risk, such as the risk of a computer virus that emails patient data
  - Project risk is the risk that the remediation plan selected cannot be completed.
  - Both are valuable
- Continuous process required

Understanding the Components of Risk

Threat

- Threats are actions or events which might violate the security of an environment
- There are three components of threat
  - Targets
  - Agents
  - Events

Targets

- The target of a threat is one of the security services
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
- The target corresponds to the motivation behind the threat
- A threat may have multiple targets

Assets as potential targets

- Information
- Hardware
- Software

- Facilities
- People
- Documentation
- Supplies

- Any of these assets have varying value to your mission

Agents

- An agent of threat is an individual who wishes to do the harm
- To be a credible threat, an agent must have three characteristics
  - Access
  - Knowledge
  - Motivation

Potential Agents

- Employees
- Ex-Employees
- Hackers
- Commercial Rivals
- Terrorists

- Criminals
- General Public
- Vendors
- Customers
- Visitors
- Disasters

Some Statistics

- In 2001, half of companies had their web servers attacked
- Almost 90% percent experienced worms, viruses, or Trojans
- Almost 40 percent suffered denial of service attacks,
- Nearly 1/3 faced buffer overflow attacks
- Cyber-terrorism is on the rise

But …

- The overwhelming majority of security breaches are internal
  - A key risk is that your users don’t understand their responsibilities well enough to cooperate with your guidelines
  - Disgruntled employees are a major risk. Not all are ex-employees

Events

- Events are the mechanism that an agent can cause the harm
- The event must cause the appropriate harm to the target
- The agent must have the appropriate knowledge and access to perform the event

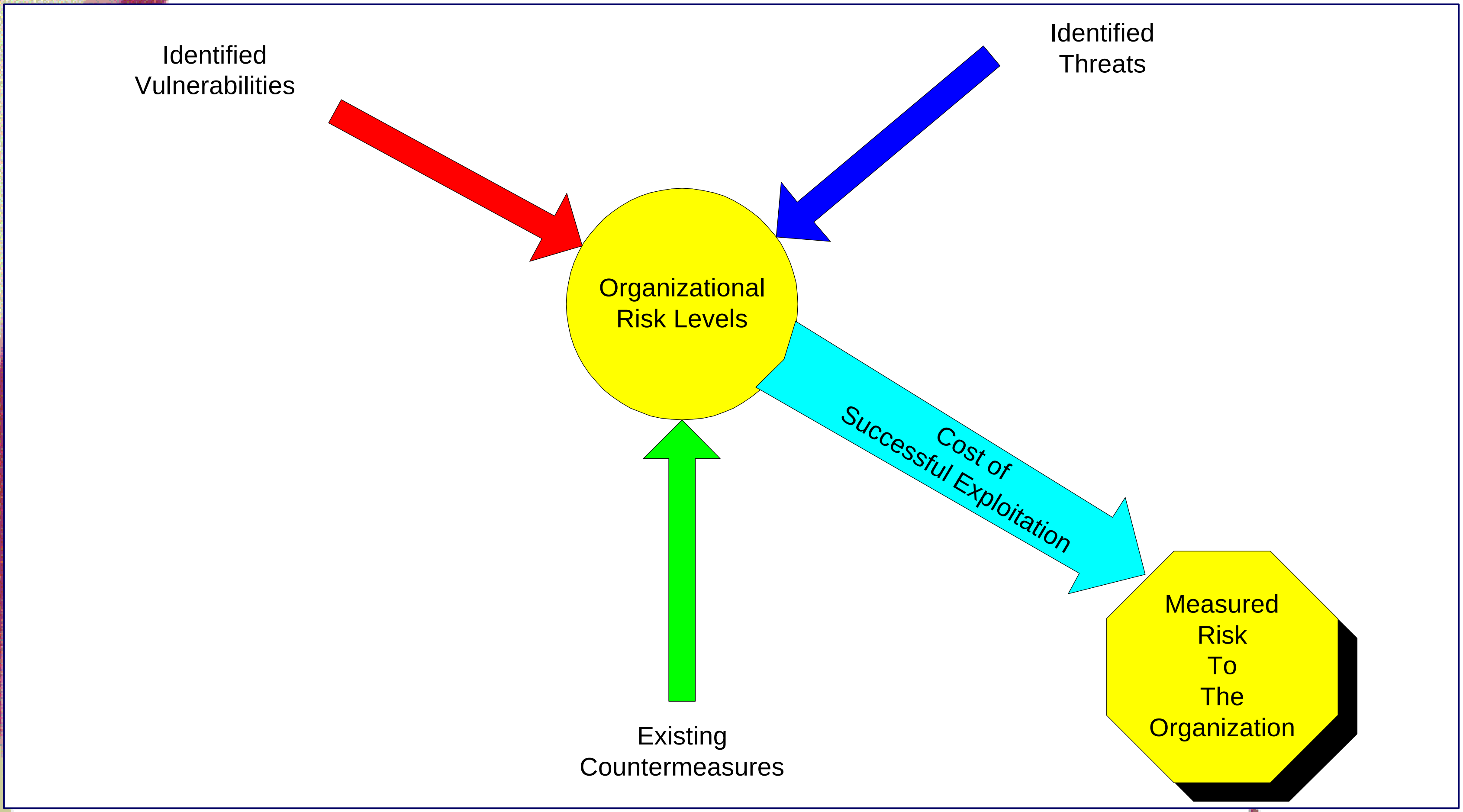
Potential Events

- Misuse of authorized access
- Malicious alteration of information
- Accidental alteration of information
- Unauthorized access
- Malicious destruction
- Accidental destruction
- Malicious physical interference
- Accidental physical interference
- Natural physical events
- Introduction of malicious software
- Disruption of communications
- Passive eavesdropping
- Theft

Countermeasures

- Vulnerabilities cannot be examined in a vacuum
- Countermeasures must be taken into account
  - Firewalls
  - Anti-virus Software
  - Access Controls
  - Authentication
  - Physical Security
  - Employee Training

The Big Picture


Identified Vulnerabilities
Identified Threats
Organizational Risk Levels
Cost of Successful Exploitation
Existing Countermeasures
Measured Risk To The Organization

Measuring Risk

- Existing vulnerabilities, threats, and countermeasures provide part of the story
- Risk should also be measured in terms of the harm that can be done if the risk is realized

Risk Can be Measured

- Money
  - – Real financial loss
- Time
  - – Lost time of staff or capabilities
- Resources
  - – The amount of resources needed to correct the situation
- Reputation
  - – Lost trust in the organization or business
- Lost Business
  - – Loss of potential business

The Risk Assessment Process

First, Identify all the risks

- Start with a brainstorming session
- Accept any possible risks at first
- Walk through the categories of targets, agents, and events to trigger the thinking process
- Accept people's "pet risks" without comment
- No recriminations for identifying risks

Capture enough data

- Include both condition and consequence
- Use the form:
  - – Given that … there is concern that …
  - – Example: Given that there are PCs on our network running PC-Anywhere without password protection there is concern that war dialers could penetrate our network and compromise the confidentiality of our data

Next, Process the risks

- Separate out the problems
- Separate out the “project risks”
- Combine equivalent risk statements
  - Don’t combine equivalent causes
- Group related risks
  - Index card sorting
  - Use whatever grouping is logical

Caution

- Don’t try to solve risks now
- Don’t make excuses now
- Don’t evaluate severity now

Rank the Risks

- Numbers have more force
- Allows you to identify top-N risks
- A limited set of numbers produces more relevant numbers
  - Rankings can always be refined
  - Resist the temptation to rank on a scale of 10. Use a scale of 5 and multiply by 2 if needed.

Ranking the Risks

Probability

Impact

	Low (1)	Med-Low (2)	Med-High (3)	High (4)
Critical (4)	4	8	12	16
Serious (3)	3	6	9	12
Significant (2)	2	4	6	8
Minor (1)	1	2	3	4

Adjust for countermeasures

- Adjust identified risk scores as needed to address countermeasures that already exist
- You probably have already accounted for this somewhat with your probability scores
- This step is important enough to address on it's own
- You will be asked about existing countermeasures at the board when you ask for money

Practical Modifications

- After ranking, you still may want to vote. (4-n or 5-n systems still lack some granularity)
- Have the entire committee adjust the ordered risk list

Using Risk to make decisions

Making HIPAA-confident decisions

- HIPAA mandates reasonable efforts to protect the privacy and security of individuals' information
- The solution is to get the most "bang for the buck" with the security dollars you can afford to spend (read as scrape together)
- Back up with auditing and extensive training efforts

Maximizing the Bang/Buck ratio

- Make decisions that:
  - Address known problems
  - Respond to biggest risks
  - Respond to significant risks with minimal cost to implement
  - Respond to as many issues as possible

Things to think about

- Training dollars are often the best spent dollars in the budget
- Must keep the short and long run in view at all times.
- Never lose sight of hard numbers. If you can place hard numbers behind a solution, it's salability goes way up.

Formal bang/buck evaluation

- Re-rank risks assuming that the solution is deployed
  - Watch out for increases in some areas
- Score the decrease in risk scores for each solution being evaluated vs. cost
  - May be best to evaluate cost on a simple scale
  - Don’t forget workflow costs

Taking it to the board

- Major role of the board of directors is to manage organizational risk
- Present requests for spending to address an unacceptable level of risk
- Risk “numbers” with hard data backup sell better
- Hard to say no to a spending request that addresses a top-N risk (or more than one!)

Example Decision

- Identified top-N risk: External access via non-controlled dial in.
- Solution evaluated: Strong-authentication remote connect utility
  - Inside vs. outside (other risks and business problems)
  - Expandable (short vs. long term)

Designing the Risk Management Process

The Plan

- Assess risks
- Respond to the risks
  - Technical and administrative solutions
- Reassess the risks
  - Changing environments
  - New solutions
  - Results of audits

Who

1. Senior Management (Other than CIO)
2. Security Officer
3. Chief Information Officer
4. Risk Manager
5. HIM Director or Privacy Officer
6. Compliance Officer or other Legal
7. Clinicians

Note: Doesn’t this look like your steering committee???

Team Startup Tasks

- Establish a charter
- Clearly defined scope
- Regular meeting times
- Reporting structures and formats
- Documentation tools
  - Forms
  - Minutes

First Risk Assessment

- Perform tasks from the previous risk assessment slides
- More important to develop a good process that get the results absolutely perfect

Ongoing Activity

- Regular meetings to:
  - Introduce new risks
  - Revisit existing risks
  - Evaluate remediation strategies
- Consider the effects of:
  - External changes
  - Internal changes

Conclusions

Conclusions

- Risk Analysis and Risk Management are required by HIPAA
- The risk methods represent a solid basis for quality security decision making
- Basic analysis methods are well within reach of the average covered entity

Questions?

Additional Resources

• HIPAAdvisory	www.hipaadvisory.com
• DHHS/HIPAA:	aspe.hhs.gov/admnsimp
• WEDi/SNIP Web site:	snip.wedi.org
• Transactions and Code Sets including implementation guides:	www.wpc-edi.com/hipaa
• Draft HIPAA Security Imp. Guide:	www.wedi.org
• NCHICA	www.nchica.org
• ASC X12N Standards:	www.wpc-edi.com/hipaa
• Practices:	www.mgma.com

PHOENIX HEALTH SYSTEMS
healthcare IT solutions

Any further questions?

Tom Grove, Director
Phoenix Health Systems
9200 Wightman Road, Suite 400
Montgomery Village, MD 20886
Telephone: 301-869-7300
tgrove@phoenixhealth.com