


Risk Assessment: Key to a successful risk management program



Sixteenth National HIPAA Summit

Timothy H Rearick, MBA, PMP

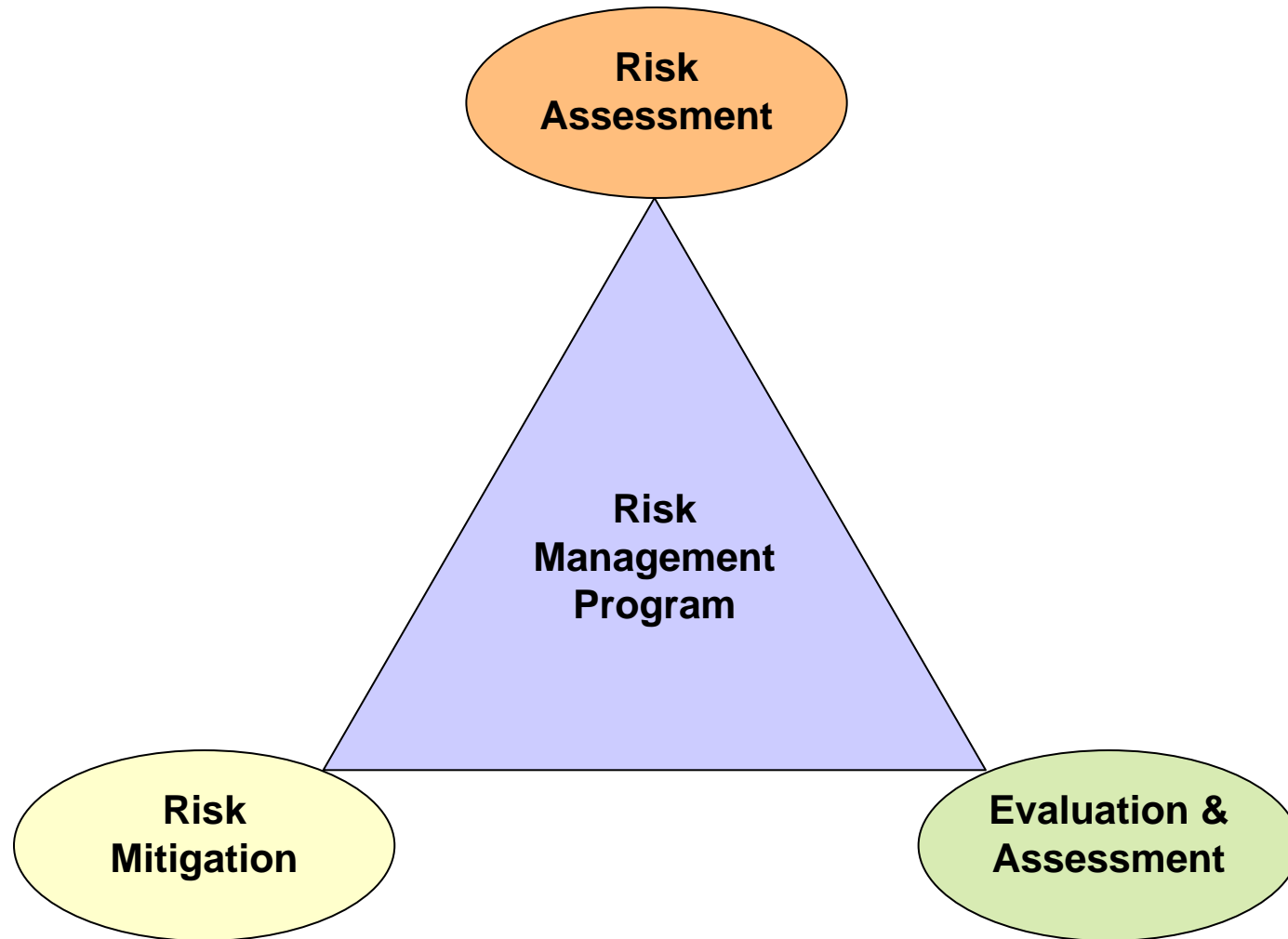
August 22, 2008



Learning Objectives

- Define risk assessment
- Why complete a risk assessment
- How risk assessments work
- Expected deliverables

Enterprise Risk Management

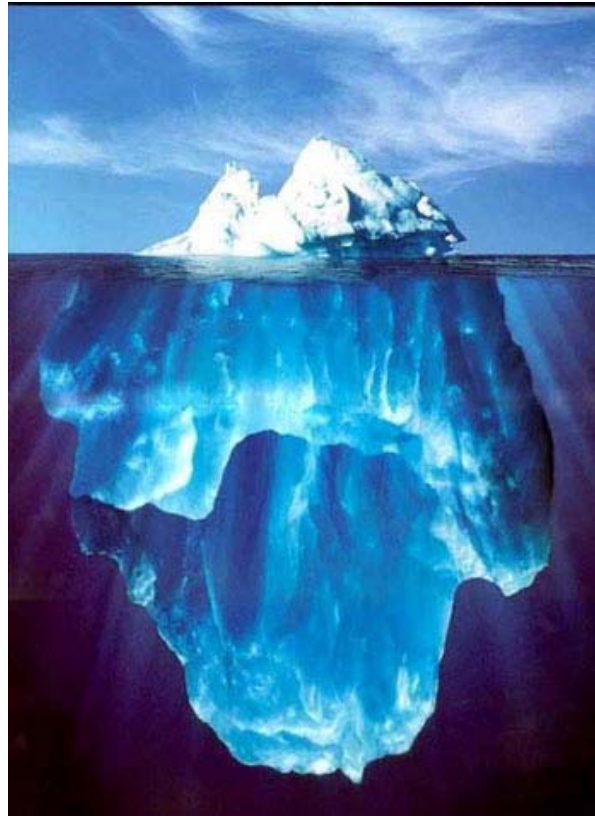




Risk Assessment Defined

- Evaluates the enterprise information security program against specific criteria (ISO/IEC 27002, NIST, etc)
- Documents threats, vulnerabilities and likelihood of damage
- Identifies defensive measures

Information Security Landscape

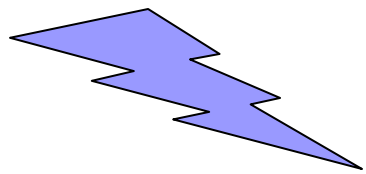




Risk Assessment Drivers

- Information security incidents
- Federal and State laws
- Legal liability
- Cost of remediating breaches

Information Security Incidents



Natural Disasters



Fraud



User Error



Sabotage



Malicious Acts

Enterprise Information Assets



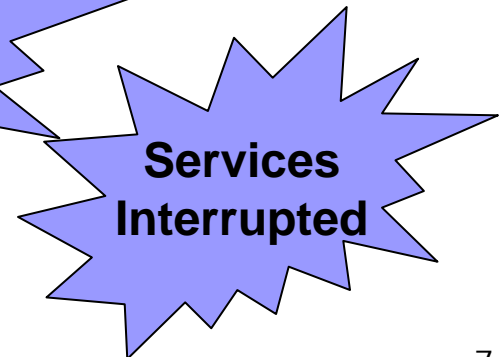
**Sensitive Data
Lost**



**Operations
Disrupted**



**Lost
Confidence**



**Services
Interrupted**



Specific Infosec Incidents

- Walter Reed Army Medical Center
- University of Florida College of Medicine
- University of Massachusetts
- New York-Presbyterian Hospital
- General Internal Medicine of Lancaster



Federal and State Laws

- HIPAA
- FISMA
- Gramm-Leach Bliley Act
- Sarbanes-Oxley
- Florida Information Resource Security Policies and Standards



Legal Liability

- Due diligence - effort made by a reasonable person to avoid harm to another party or himself
- Failure to exercise due diligence may be considered negligence



Data Protection Costs Less

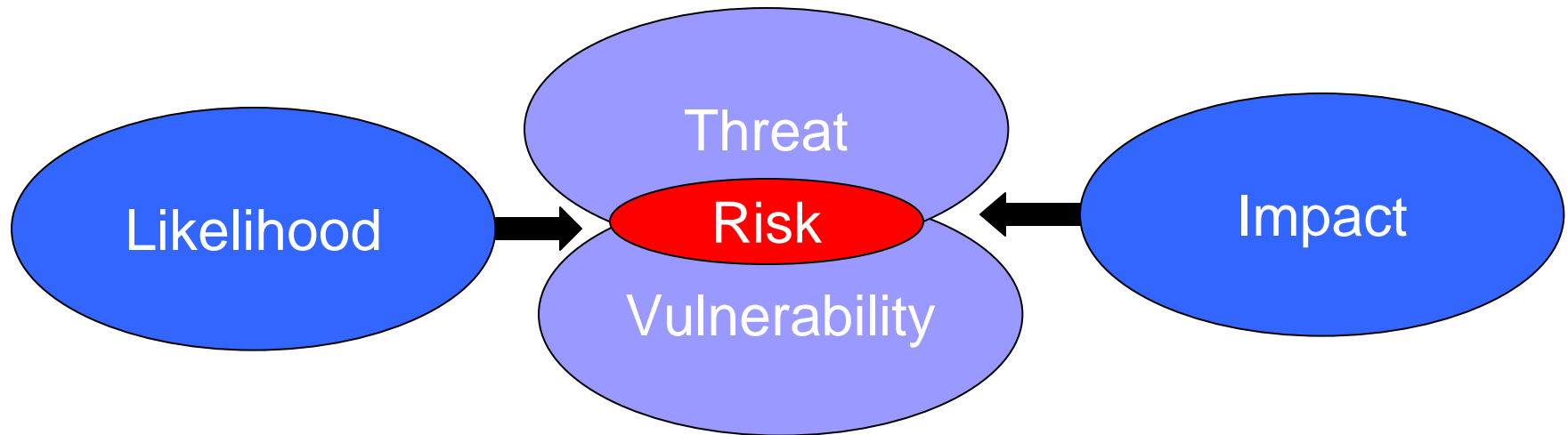
- Gartner Research 9-16-2005
 - Protecting customer data costs less
 - \$6-\$16/account to protect
 - \$90/account to mitigate a breach
- Ponemon Institute© & PGP Co Study 11-07
 - Estimate mitigation cost at \$197/record



Types of Assessments

- ISO/IEC 27002:2005
- NIST
- HIPAA
- CoBit
- NSA IAM

Concept of Risk





Risk Assessment Process

1. System characterization
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Likelihood determination



Risk Assessment Process

6. Impact analysis
7. Risk determination
8. Control recommendations
9. Results documentation



Risk Assessment Process

■ System characterization

- Hardware, software, system interfaces
- Data and information
- People (users and IT staff responsible for system)



Risk Assessment Process

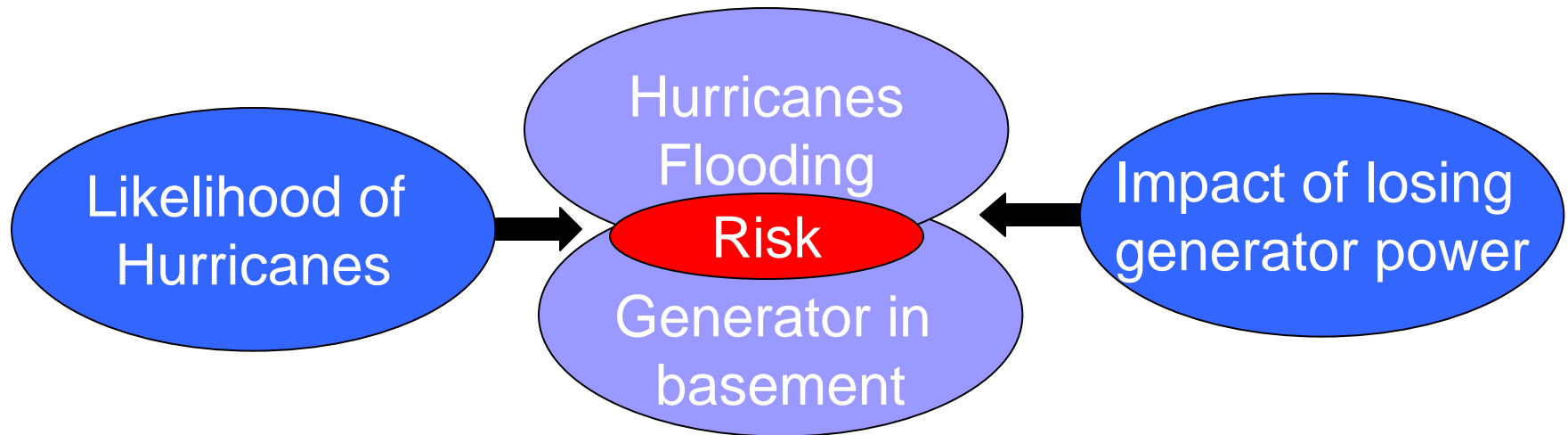
- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination



Risk Assessment Process

- Impact analysis
- Risk determination
- Control recommendations
- Results documentation

Threat Identification Example



Risk Level Matrix

	Impact		
Threat Likelihood	Low (10)	Moderate (50)	High (100)
High (1.0)	$10 \times 1.0 = 10$	$50 \times 1.0 = 50$	$100 \times 1.0 = 100$
Medium (0.5)	$10 \times 0.5 = 5$	$50 \times 0.5 = 25$	$100 \times 0.5 = 50$
Low (0.1)	$10 \times 0.1 = 1$	$50 \times 0.1 = 5$	$100 \times 0.1 = 10$

Risk Determination

- Risk level = Likelihood of a hurricane (.10) x Impact of losing the generator (100) = 10
- Risk scale >10 (low), 10-50 (medium), >50 to 100 (high)



Project Deliverables

- Statement of Work
- Project Plan
- Information System Identification Guide
- Criticality Matrix
- Final Report



Critical Success Factors

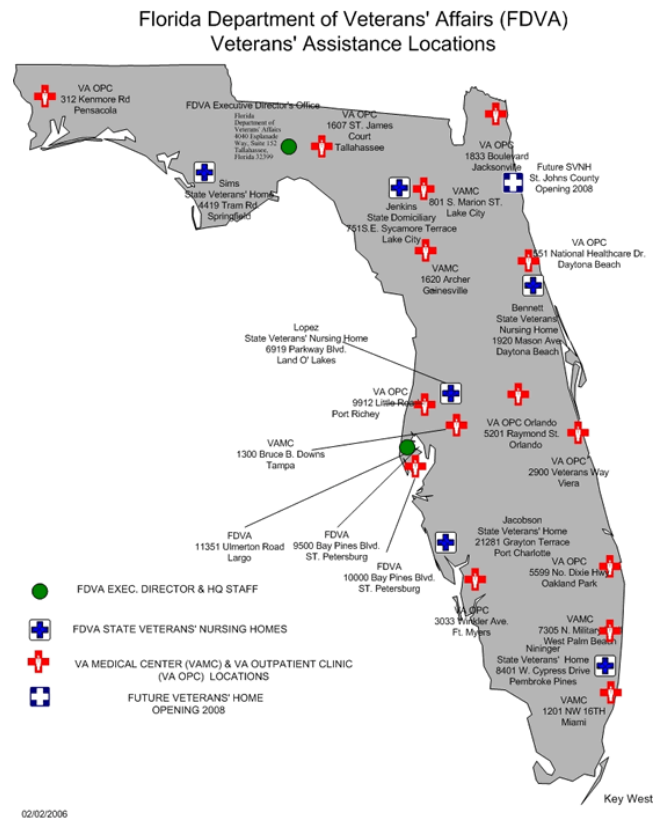
- Senior executive support
- Full support/participation of IT Team
- Competent risk assessment team
- Awareness/cooperation of the user community
- On-going evaluation and assessment of the IT related mission risks




Case Study - FDVA

- Florida Department of Veterans' Affairs
 - Cabinet Agency serving 2 million veterans
 - Veterans Benefits and Assistance Division
 - State Veterans' Homes Program
 - Operating budget of \$71,000,000
 - 647 FTE

FDVA Locations





Case Study - Approach

- Funded by Homeland Security grant
- NIST 800-30 methodology
- Issued Request for Proposal
- Met Federal and State requirements



Case Study - Value

- Comprehensive
- Independent
- Demonstrated commitment
- Validation



Case Study - Findings

- Five key recommendations
 - Physical security
 - Continuity of Operations Plan (COOP)
 - Systems testing/development
 - Systems input/output procedures
 - Policies and procedures



Case Study - Remediation

- Added security personnel
- Revised COOP
- Separated testing/development from production
- Documented systems input/output procedures
- Reviewed and revised policies and procedures

For More Information

- National Institute of Standards and Technology (Computer Security Division) <http://csrc.nist.gov/>
- HIPAA Security Standard <http://www.cms.hhs.gov/securitystandard/>
- ISO/IEC 27002:2005 Information security standard <http://www.iso.org/>



Questions & Answers

- For Further Information Contact

- Timothy H. Rearick

- 850-339-9094

- trearick.ac@northhighland.com