Business Continuity Management
5 Practical Best Practices

by Miguel O. Mercado, CISA, HiTrust Practitioner

June 28, 2016

2016 Atlantic Hurricane Season

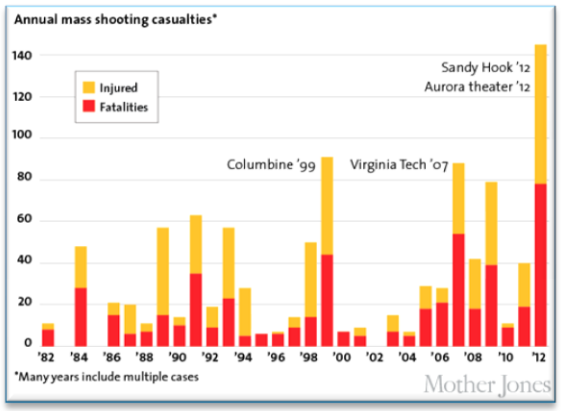
- **From**: June 1
  To: November 30
- **NOAA Forecast:**
  - Near-normal Atlantic hurricane season is most likely this year.
  - 70% likelihood of 10 to 16 named storms

Predictions of tropical activity in the 2016 season

Source	Date	Named storms	Hurricanes	Major hurricanes
Average (1981–2010[1])		12.1	6.4	2.7
Record high activity		28	15	7
Record low activity		4	2†	0†
TSR[2]	December 16, 2015	13	5	2
TSR[3]	April 5, 2016	12	6	2
CSU[4]	April 14, 2016	13	6	2
CCU[5]	April 15, 2016	13	7	4
NCSU[6]	April 15, 2016	15–18	8–11	3–5
UKMO[7]	May 12, 2016	14*	8*	N/A
NOAA[8]	May 27, 2016	10–16	4–8	1–4
TSR[9]	May 27, 2016	17	9	4
CSU[10]	June 1, 2016	14	6	2
WT[11]	June 1, 2016	14	9	3

Source: https://en.wikipedia.org/wiki/2016_Atlantic_hurricane_season

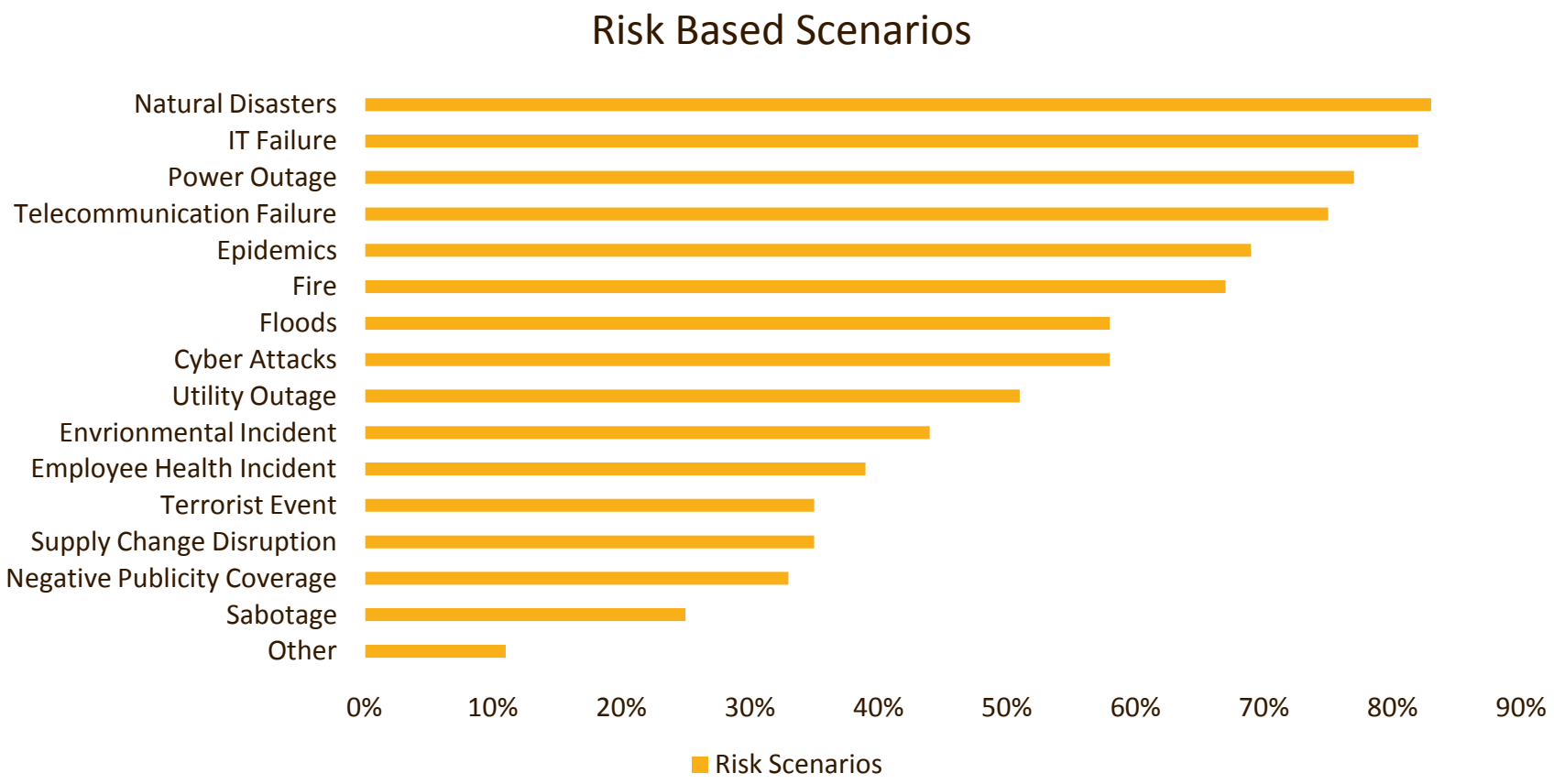
Emergency and Disaster Examples



Lesson #1: Use Risk Based Scenarios

- Develop Business Continuity Plans (BCP) that address different types of emergency and disaster scenarios.
- One generic plan can not cover all scenarios!!!

Examples of Scenarios to Consider



Survey #1: Choosing Your Scenarios

Lesson #2: Choosing Your Scenarios

- Must be part of your Business Continuity Management (BCM) risk assessment process.
- The risk assessment process should help your organization:
  - Identify potential *Threats*.
  - Assess the *Likelihood* of each *Threat*.
  - Determine potential *Impact*.
  - Calculate level of *Risk*.
  - Identify the key priority areas.

Determining Level of Risk

- There are many ways to determine the level of risk:

Likelihood (Threat event occurs and results in adverse Impact)	Level of Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

- What is important is that you follow your organization risk management framework.

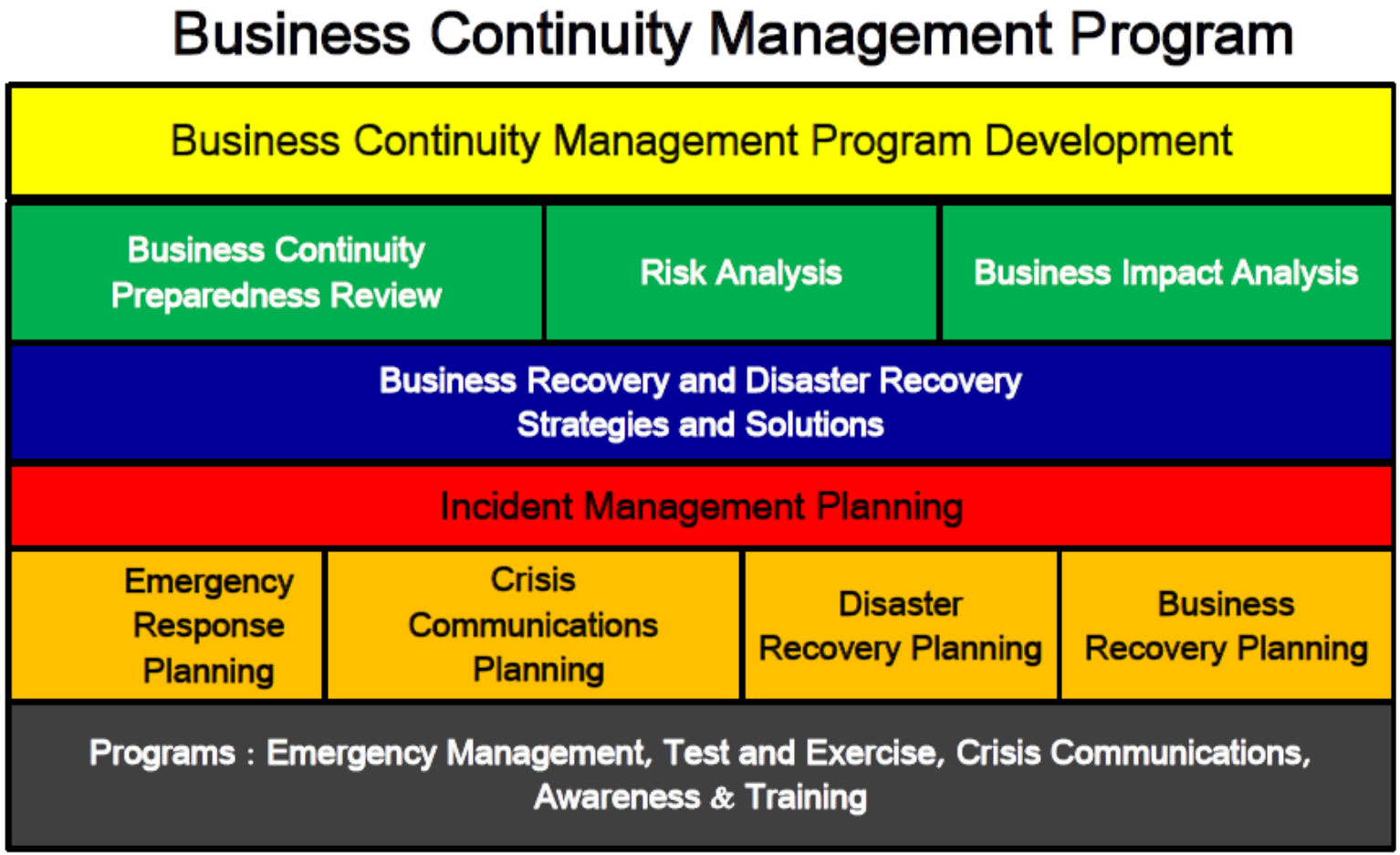
Survey #2: Is your organization ready?

Is your organization ready to manage a major disaster?

Will the organization be able to recover mission critical business processes?

☐ Yes ☐ No ☐ Not Sure

Lesson #3: Potential impact to the organization will increase if an ad hoc process is followed



Survey #3: Most critical component to implement

- After a Business Continuity Management Program what is the most critical component to implement?
  a) Communicating to management results
  b) Conducting employee awareness
  c) Conducting simulation and testing exercises

Lesson 4: Conducting validation and testing exercises is a critical component

- Business Continuity (BC) require regular testing and validation:
  - *Testing* is an activity that is performed to evaluate performance, capabilities or properties relative to specified measurement criteria;
  - *Validation* is an activity that is performed for the purpose of corroborating soundness, completeness, or effectiveness

Note: For simplicity, we will refer to both types of activity as 'tests'

Lesson 4: Conducting validation and testing exercises is a critical component

- Test and Exercise Program Objectives:
  1. To evaluate the functionality of the current corporate continuity program.
  2. To identify the areas of opportunity or lack of information within the current corporate continuity program.
  3. To ascertain what premises within the continuity planning should be reviewed, modified and updated.
  4. To provide information and increase confidence between the participants.
  5. To develop effective teamwork.

Lesson 4: Conducting validation and testing exercises is a critical component

- Test and Exercise Program Objectives:
  6. To increase the level of knowledge when performing tests and exercises within the organization.
  7. To measure the level of effectiveness and optimize the business recovery times of critical processes; and to preserve the operational continuity of all critical business.

Survey #3: What Must be Tested?

1. Manual procedures
2. Automated procedures
3. Backup and recovery configurations (DRP)
4. Call trees (Incident Management)
5. Contact lists, resource lists, off-site inventory lists, etc.
6. All of the above.

Lesson #5: Comprehensive Testing Plan Required

- Testing & Validating BC Plans
  - All manual procedures
  - All automated procedures
  - All backup and recovery configurations (DRP)
  - All call trees (Incident Management)
  - All contact lists, resource lists, off-site inventory lists, etc.
- In other words, every single component of your plans!

When Should You Test?

- Every component should be tested at least annually.
- Critical and/or highly volatile components should be tested at least quarterly and after any major technological change.
- Call trees should be tested at least semi-annually and after any major organizational change.
- Components which fail a test should be re-tested as soon as possible.

Example of Exercise #1

- Contractor conducting remodeling work in floor 4 accidentally breaks a water pipe.

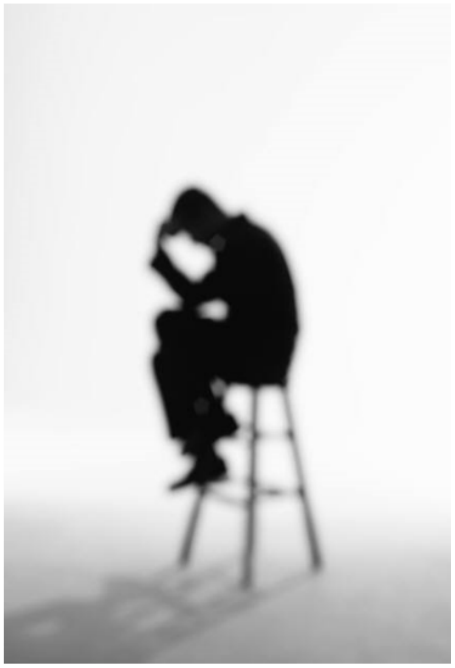
Monday
10/20 @ 10:00 AM

Incident: Water damage

Conclusions

1. Consider and plan for multiple scenarios.
2. Identify your most relevant scenarios based on the results of your Business Continuity risk assessment process.
3. Potential impact to the organization will increase if an ad hoc process is followed. Formalize your BCM program,.
4. Testing and validation is the most critical component to implement.
5. Comprehensive testing plan required.

Q&A



Thanks!