BP17: To BIA or Not to BIA

Roger Stearns, MBCI, CBCP, CHS-III
Ever Vigilant Consulting LLC

CPM 2009 WEST

Do Nothing

“Even if you’re on the right track, you’ll get run over if you just sit there.”

- Will Rogers

Roger Stearns, MBCI, CBCP, CHS-III

- Owner/Consultant – Ever Vigilant Consulting LLC
- 24 Years working in Emergency, Business & Disaster Mgmt.
- Public, Private, Government, DOD, Military
- USA, Canada, South America, UK, Europe, India, Japan and Australia
- Banking, Financial, Catering, Livery, Farming, Insurance, Call Centers, Off-Shoring, Software, Telecom, Data Centers, Security, Benefits, HR, and Risk to name a few.

Stated Objectives

- How to determine the right scale of Business Impact Analysis for your organization.
- To explore probability models and risk assessments and decide when to use them.
- When to choose a "do nothing" strategy

Overview

- Doing nothing at all
- Choosing to do something
- Deciding to do nothing

DO NOTHING AT ALL

IT IS ASSESSED THAT 50% OF BUSINESSES EXPERIENCING A DISASTER AND HAVING NO EFFECTIVE PLAN FOR RECOVERY WILL FAIL WITHIN THE FOLLOWING 12 MONTHS

Headlines

- “40% of all small businesses will go out of business if they cannot get to their data in the first 24 hours after a crisis.”

- Gartner

Headlines

- “43% of companies never resume business following a major fire. Another 35% are out of business in the following three years.”

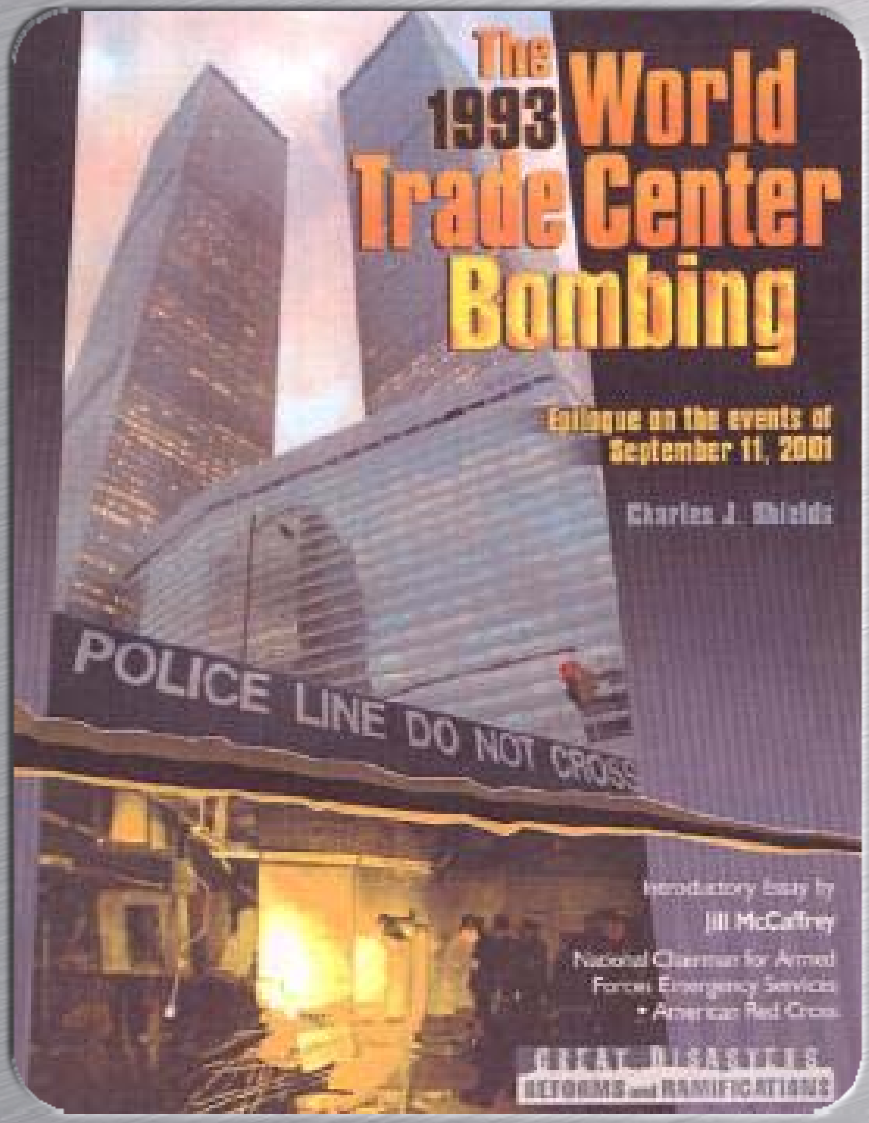
- US National Fire Protection Agency

Headlines

- “Many companies often spend more time planning their company picnic than for an event that could put them out of business.”

  - Epoch 5

1993 WTC Bombing



- 450 Companies Impacted
- 147 were non-recoverable
- Majority were out of business in 1994

September 11th, 2001

- 800+ companies impacted
- 250 disaster declarations
- 150 out of business by 2002

Hurricane Katrina 2004

- 25% of the small businesses went out of business
- = 20,000 business +/-

Those who plan tend to fare better than those who don’t

“By failing to prepare you are preparing to fail”
- Ben Franklin

Large scale disasters are becoming more frequent!


BROOKLYN DAILY EAGLE

WALL ST. IN PANIC AS STOCKS CRASH

Attempt Made to Kill Italy's Crown Prince

Hollywood Fire Destroys Films Worth Millions

High Duty Group Gave $700,000 to Coolidge Drive


Sun-Sentinel

ORTS: Orioles' Ripken signs $32.5 million, 5-year deal. 1C

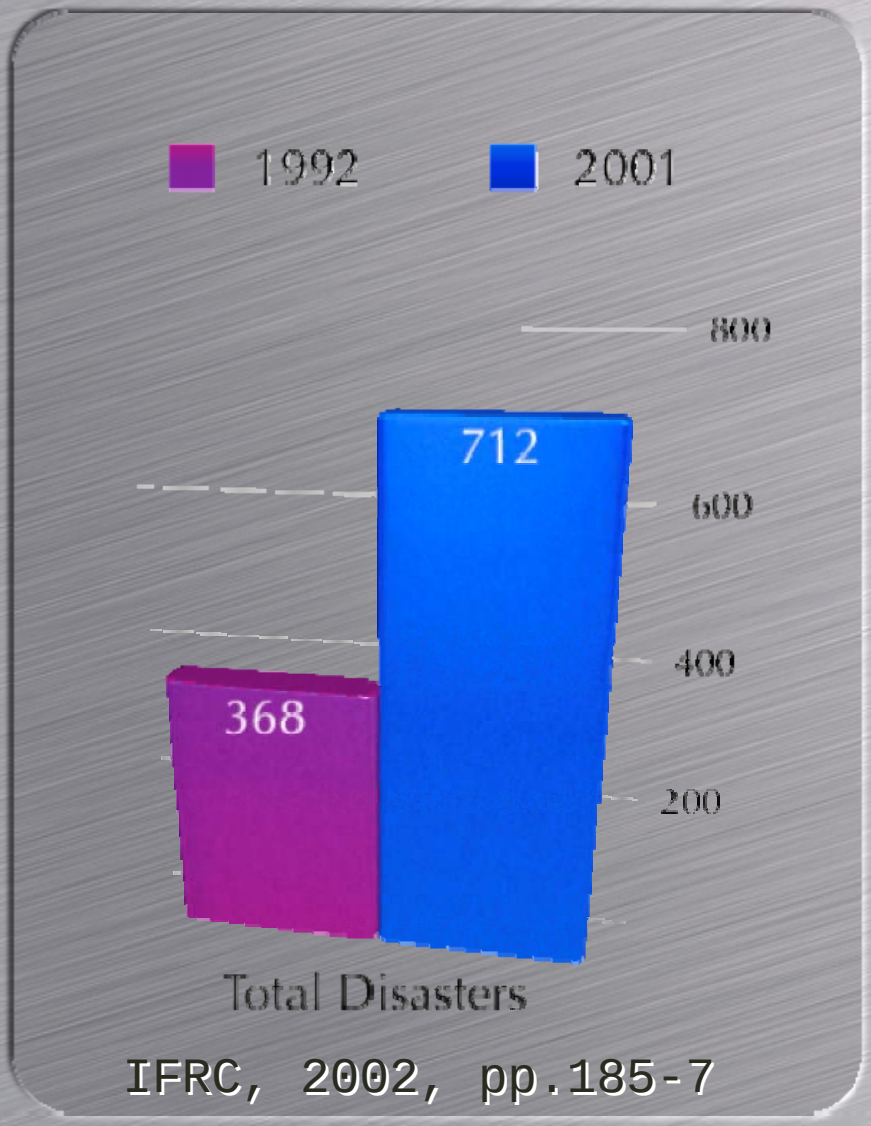
ath of terror

Andrew wreaks havoc in S. Florida

15 die; cost in billions

Dade residents stunned as storm shatters lives

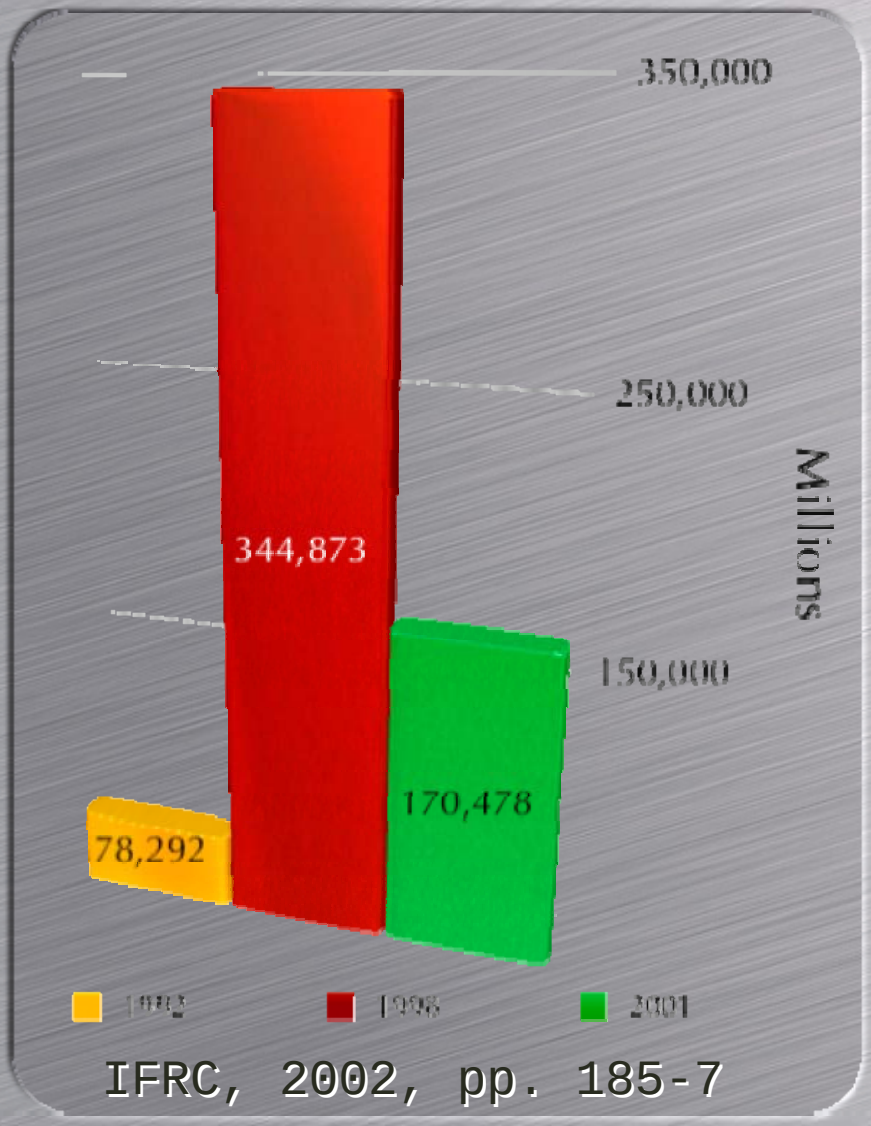
Disasters



IFRC, 2002, pp.185-7

- 93%
- Over a decade

People Impacted



IFRC, 2002, pp. 185-7

- Spike in 1998
- 45% increase over decade
- Non stereotypical Vulnerability

Potential Factors

- CNN Effect
- Increase in “Disaster Cycle”
- Numerically more events
- Lower Thresholds, Higher Expectations

“Disaster Cycle”

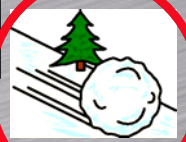
People see risk as no cost/loss option.

Flood in Town “A” - 1970

DISASTER

Disaster Relief

Disaster Recovery/ Repair/ Replace



People see risk as no cost/loss option.

Flood in Town “A” - 1990

DISASTER

People see risk as no cost/ loss option.

Disaster Recovery/Repair/ Replace

Disaster Relief

Flood in Town “A” - 2000

DISASTER

Disaster Recovery/Repair/ Replace

Disaster Relief

Choosing to do something

Are you compelled to do anything?

- NO. However, it would be recommended that you check with your insurer to see if they require you to or a governing regulation may require you to.

There are no magic bullets

One size does not fit all

Small - Medium - Large Scale & Industry

Business Continuity Management

1. Policy Statement
   - Program Standards
   - Define RA & BIA
2. Risk Analysis
3. BIA
   - ID Products & Services
   - MTPOD, Priority
4. Recovery Strategy Development
5. BRP
6. IMP, Crisis Mgmt.
7. Notifications / Call Trees
8. Plan Sign-off
9. Training, Testing & Validation
10. Reporting

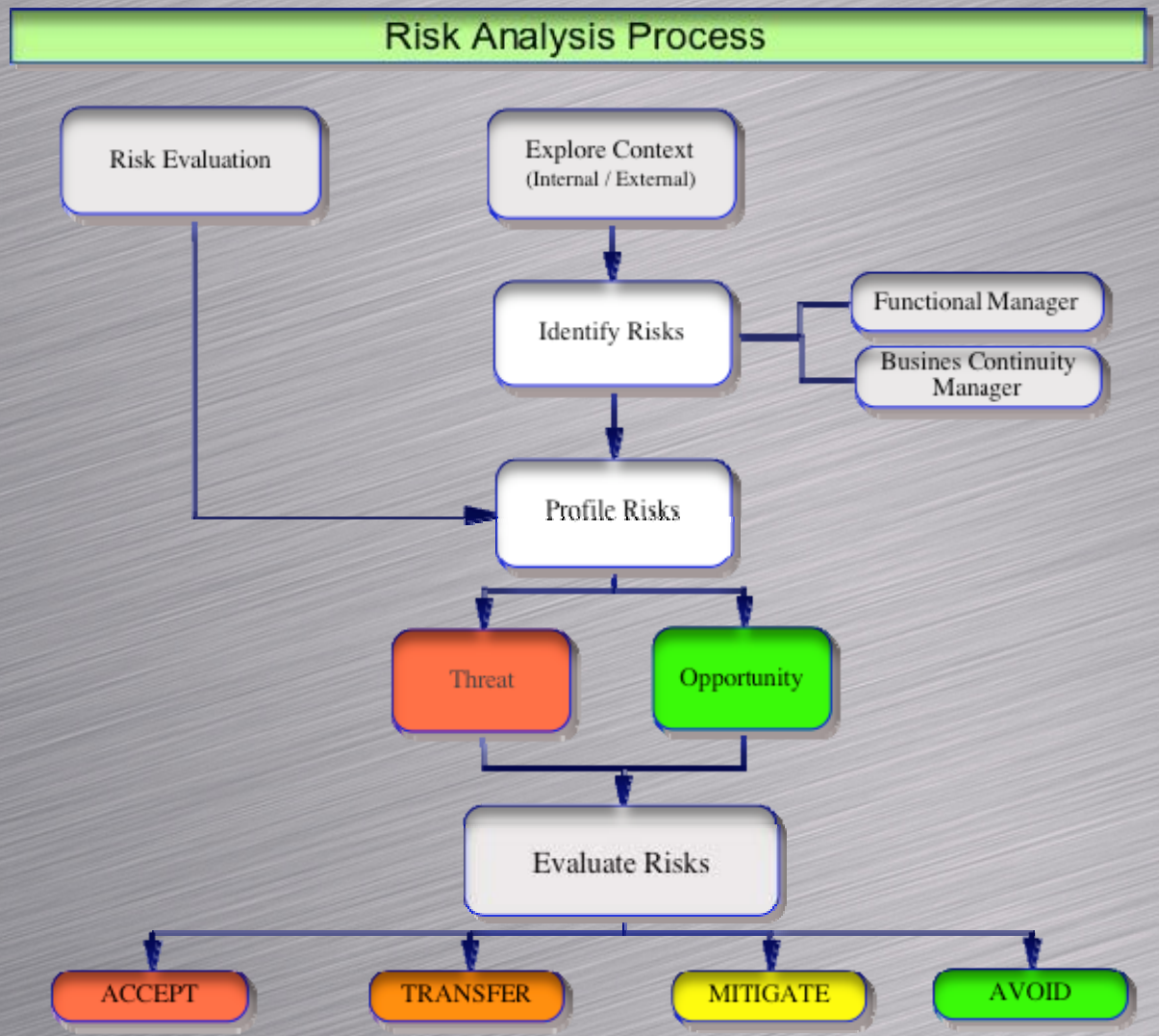
Risk Analysis
“Threat Vulnerabilities”

- Common Methodologies
  - Risk Analysis
  - FMEA
  - SWOT Analysis

Risk Analysis

- A risk analysis is one of the first steps in building a business continuity plan and program. The analysis should be conducted with key business stakeholders and the business continuity planner to identify all likely areas of risk.
- Possible threats to business continuity can be external or internal and can be natural, technical or human related. Even though it can be difficult to determine the exact nature of potential failures, it is important that risks be assessed and if possible quantified.

Risk Analysis



Risk Analysis

Step One: Detect & Classify Risks

Preventable Emergencies

- Building location
- Age of infrastructure
- Employees
- Security Measures

Unpreventable Emergencies

- Crime
- Severe weather
- Communications failures
- Civil disturbances

Step Two: Quantify those risks

(Probability of occurring)

Hazard Vulnerabilities Analysis Chart						
Type of risk	Historical Occurrence	Probability of Occurring	Human Impact	Property Impact	Business Impact	Total

FMEA

Failure Mode & Effect Analysis

- Identify, assess and address the potential failures of a process, service or system
- Helps in determining redundancy
- Increases the likelihood that all reasonable threats will be considered
- Identifies potential vulnerabilities and their interdependencies
- Recommended by the ISO

FMEA

Continued

Types of FMEA's

- FMEA's focused on minimizing failures of a:
  - System
  - Design
  - Process
  - Service
- FMEA's that attempt to maximize quality, reliability and the maintainability to:
  - System
  - Design
  - Process
  - Service

SWOT

Strengths, Weaknesses, Opportunities & Threats

- **The SWOT Analysis matches resources and capabilities.**
  - **Strengths** - Internal resources and capabilities
  - **Weaknesses** - Internal absence of strengths
  - **Opportunities** -May be revealed by external analysis
  - **Threats** - Changes in the environment may lead to threats

SWOT

Continued

	STRENGTHS	WEAKNESSES
OPPORTUNITIES	S - O STRATEGIES	W - O STRATEGIES
THREATS	S - T STRATEGIES	W - T STRATEGIES

- **S - O STRATEGIES : Pursue opportunities that align with strengths**
- **S - T STRATEGIES : Strengthen weaknesses in order to pursue opportunities**
- **W - O STRATEGIES : Use strengths to reduce vulnerabilities**
- **W - T STRATEGIES : Create a plan that prevents weaknesses from creating vulnerabilities**

Business Impact Analysis "The BIA"

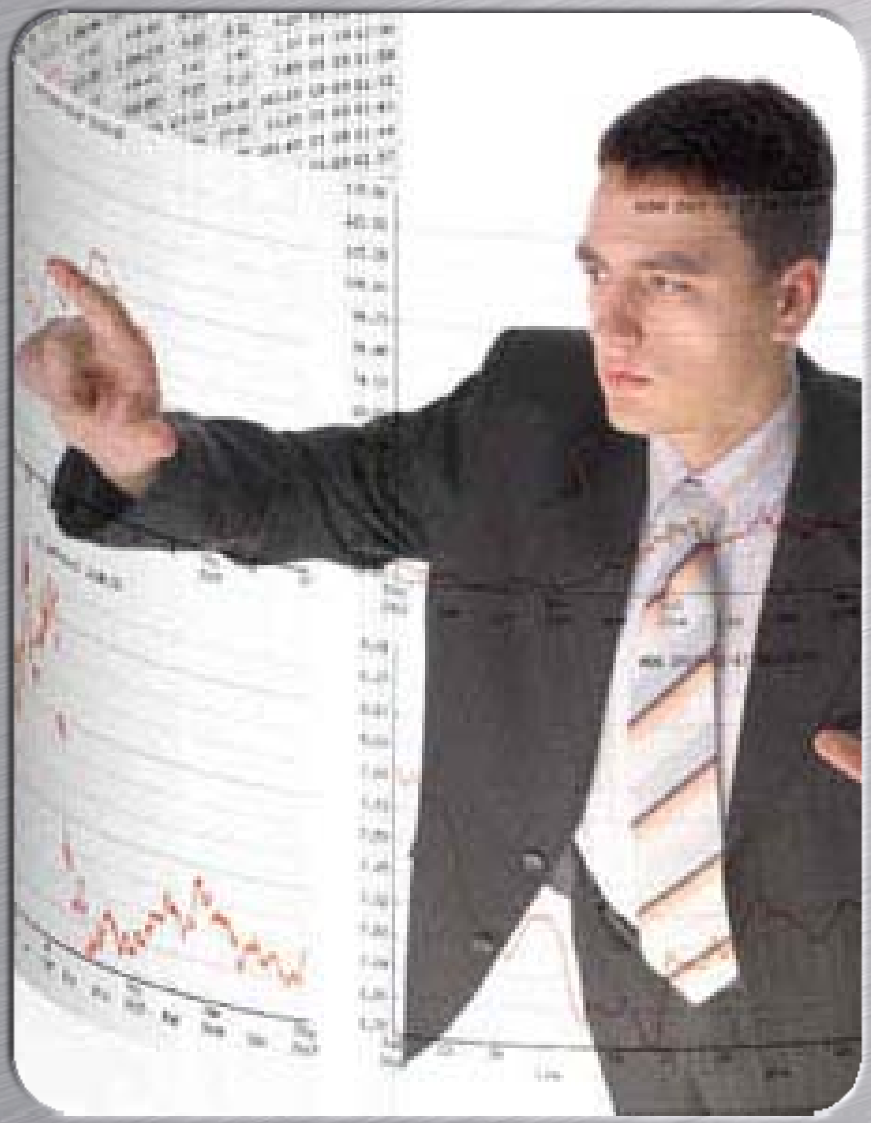
- Define Critical Activities/Functions
  - Who, What, Where, When, How
  - Identify Dependencies & Interdependencies
  - Vital records, Critical Applications/Software
- Set Priorities (Who's first on the list) based on critical recovery times.
- Identify potential strategies based on Risk Analysis
  - Process recovery
  - Technology Recoveries (Network, ISP, Telephony)

BIA CONT.

- Things to consider
- Scope
- How in depth do you go?
- What will you do with the data?

The Decision to do nothing.

Risk Assessment



- ACCEPT
  - Do Nothing
- REJECT
  - Change, suspend or terminate
- TRANSFER
  - Outsource partner
- MITIGATE
  - Business Continuity measures

Do Nothing Rationales

- **Recovery Time Objective (RTO) too long for situation/event.**
  - **Situation is hours in duration, 1 day and recovery solution takes longer than typical disruptions.**

Do Nothing Rationales

- Managers unfamiliar with recovery strategies go to "Plan B". (Make it up as you go).
- Leading to Critical Function/Activity was not rated correctly from the beginning.

Do Nothing Rationales

- Incident averted
  - Civil unrest
  - Convention cancelled
  - Power restored
  - Storm changed path

Do Nothing Rationales

- **Catastrophic event**

(Katrina, 9-11 type events)

Do Nothing Rationales

- **High Probability, Low Impact**
  - Normal regional weather events (Snow/ice)
  - Use solutions like “Hoteling” that are case by case driven

Be Aware of geographical probability dissimilates

Do Nothing Rationales

- **Low Probability, High Impact Event**
  - **WHO Phase 6 - Pandemic ?**

Be Aware of geographical probability dissimilates

Do Nothing Rationales

- **Cost-Benefit (Too expensive)**

Do Nothing Rationales

- Rely on Insurance
  - Business Interruption Insurance
  - Reinsurance
  - Self-insure
  - SBA Loans
  - NHIP / Earthquake Insurance
  - Property Insurance

Tangible vs. intangible or Hard vs. Soft dollars

The Question

When is it right for YOU to

DO NOTHING?

Contact Information

Roger Stearns, MBCI, CBCP, CHS-III

Owner/Consultant

Ever Vigilant Consulting LLC

Email: rstearns@evervigilantconsulting.com

Phone: +1 603.487.3090

Web: www.evervigilantconsulting.com