

irwin siegel agency, inc.  
INSURANCE PROGRAMS & RISK MANAGEMENT

# Preparedness in Today's World

# AGENDA

P  
R  
E  
D  
I  
C  
T

L  
C  
I  
D  
E  
R  
S

P  
L  
A  
N

N  
I  
V  
E  
R  
S

P  
E  
R  
F  
O  
R  
M

W  
O  
R  
K  
S  
H  
O  
P

1

INTRODUCTIONS

2

THE WORLD WE ARE IN

3

PREPAREDNESS: PREDICT.PLAN.PERFORM

4

NEXT STEPS

# DISCLAIMER

This presentation is not complete without the accompanying oral comments and discussion.

Any work product provided by Firestorm must be read in conjunction with all guidance given by national, state and local authorities, as well as your organization's legal counsel and regulators.

Moreover, the information given and comments made in this presentation should not be interpreted as legal advice or legal opinion.

# INTRODUCTIONS

**Brad Storey, MSW**  
Vice President, Risk Management Division  
Irwin Siegel Agency, Inc.



M.S.W, Administration, Policy and Planning  
from Rutgers University

Former safety officer for a community mental  
health center.

National speaker on Proactive Risk Assessment

NYSDOL Workplace Safety Certified Inspector  
ICR 60

# INTRODUCTIONS

Suzanne Loughlin, Esq.  
Co-Founder, Chief Risk Officer  
Firestorm Solutions, LLC



- Licensed attorney
- Former Insurance Company Executive, Managing Attorney and Litigator
- Association Threat Assessment Professionals- Member
- FEMA- Professional Development Certification
- Co-author of the book [Disaster Ready People For A Disaster Ready America](#).
- Extensive experience in risk and threat assessment, crisis management, workplace violence, communicable illness, emergency response, and crisis communications planning.

# *THE WORLD WE ARE IN*



9/11. Katrina. Virginia Tech.  
Newtown. Hurricane Sandy.  
San Bernardino.

These are not the worst disasters you will see

**The worst disaster you will see is  
the one that happens to  
you or your business**



# ATTRIBUTES OF A CRISIS OR DISASTER

- Escalating Flow of Events
- Insufficient & Wrong Information
- Intense Scrutiny
- Loss of Command and Control
- Brand & Reputation Under Attack
- Leadership is engaged personally

cri•sis

/'kr̩sɪs/ NOUN

1. A risk event for which one has not identified the vulnerabilities and exposures, has not developed a plan, and therefore does not know how to respond.

How You Respond Can Become Your Next Crisis

# EVERY DAY THERE IS AN ORGANIZATION LIKE YOURS IN CRISIS



## Janitor Charged In Stunning Case Of Sexual Abuse

4 arrests made after disabled man allegedly left  
in transport van

Data **breach** affects 9,700 at Md. nonprofit serving **disabled** · 2y

Someone hacked the computers of a state-licensed provider of services to the developmentally disabled and stole Social Security

## Gunmen open fire on room full of county health officials in California

Hepatitis A **Outbreak Among Adults with Developmental Disabilities** in Group Homes

**EXCLUSIVE:** Woman says her  
developmentally disabled sister was raped  
while at state-run group home

**Catholic Charities employees accused of** swiping cash from **developmentally disabled** residents

Colorado floods extensively damage homes serving the **developmentally disabled**

# *EVERY CRISIS IS A HUMAN CRISIS*



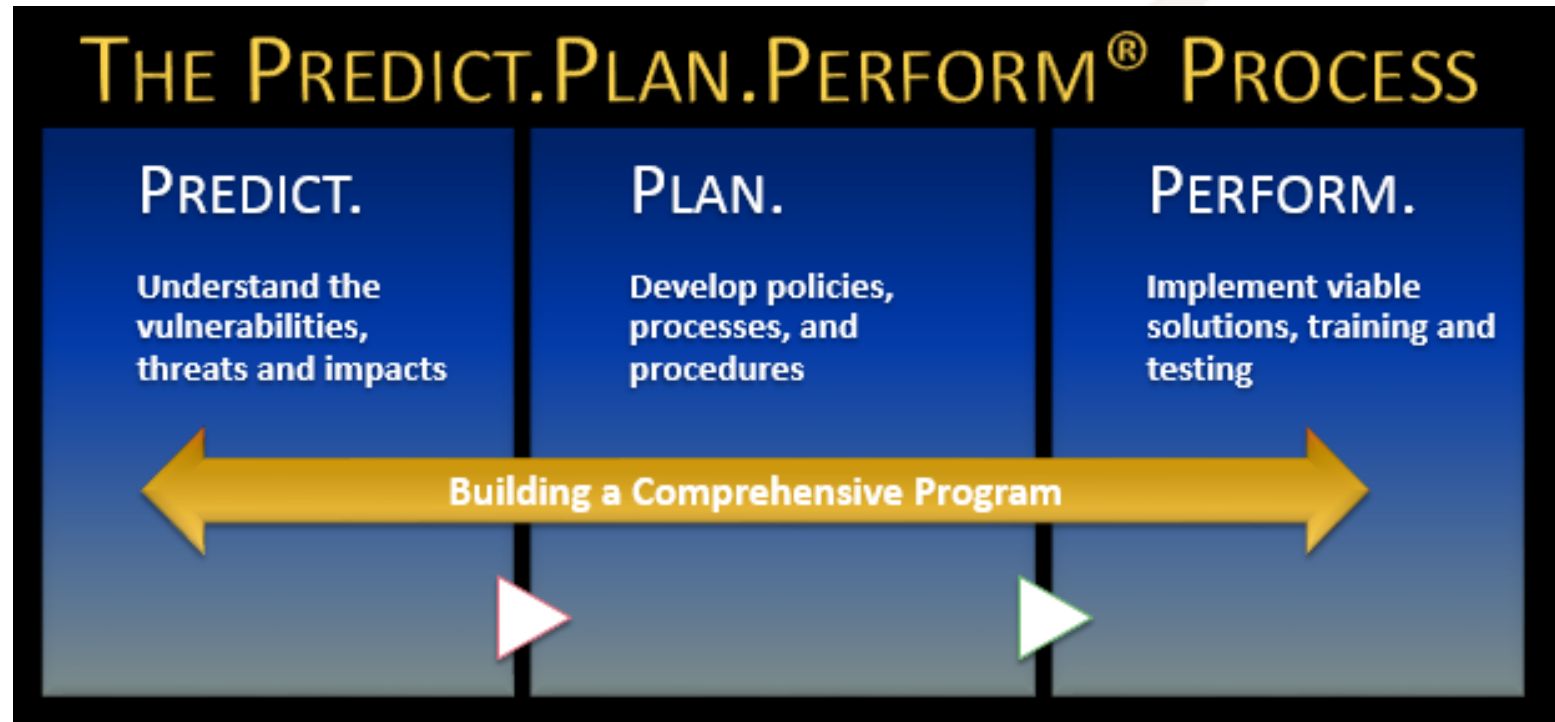
The success of any organization relies on the  
preparedness of

people

# WHAT DOES IT MEAN TO BE PREPARED?

- **Risk Assessment**— What can go wrong?
- Update or Develop **Plans**
- **Train** all Stakeholders on Plans
- Conduct **Test** Exercises
- Update and **Maintain** Program

# How Do We Get Prepared?



# PREDICT: WHAT COULD GO WRONG?

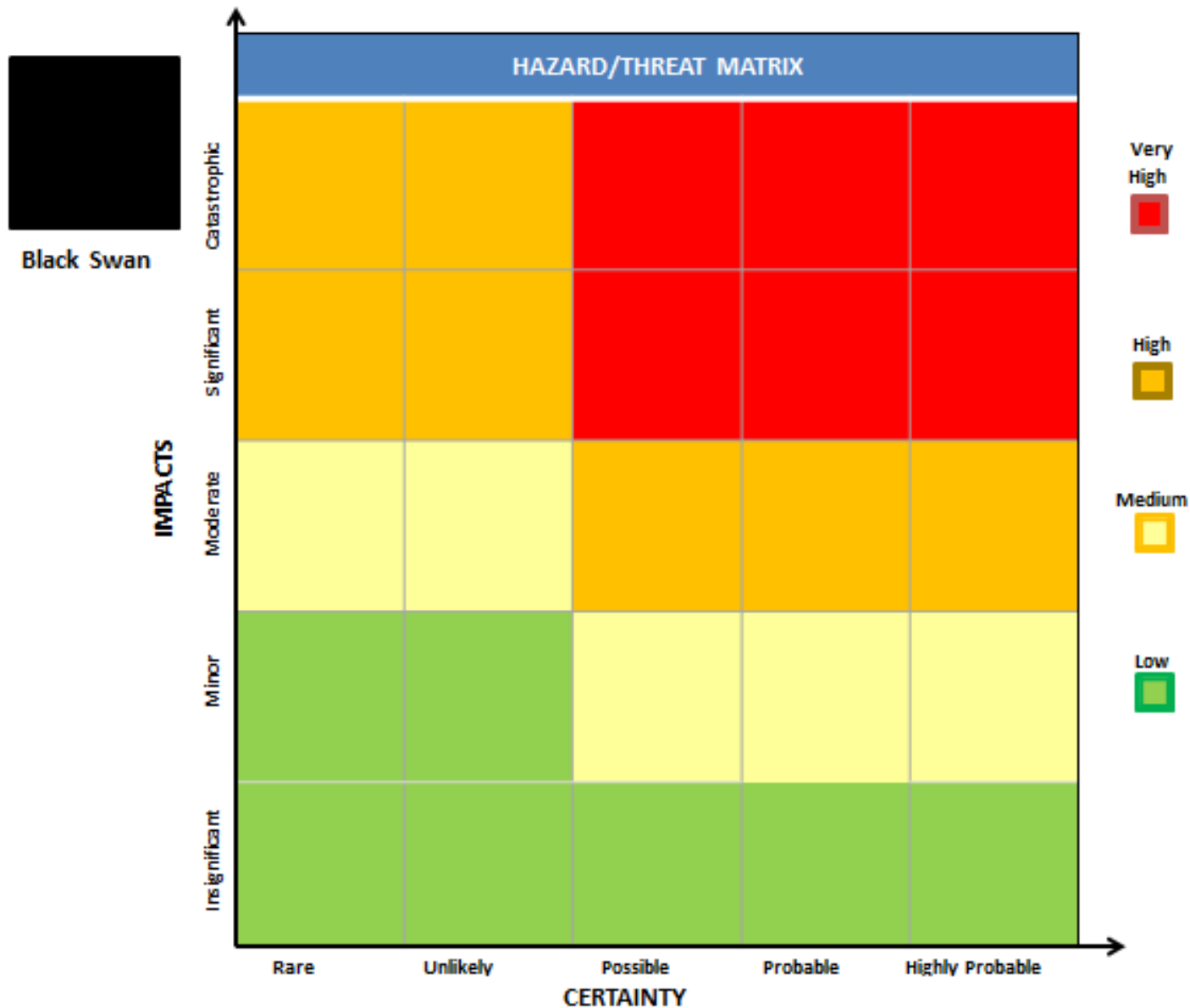
- Communicable Illness/Pandemic
- Cyber Security/Hactivist Threat (DDOS, Malware)
- Data Breach/Identity Theft
- Environmental Threats- power failure, HAZMAT,
- Ethics Violations
- Fraud
- Loss of Facility- Fire, Flood, Tornado
- Regulatory Exposures- e.g. HIPAA
- Sexual / Physical Abuse
- Social Media Risk
- Terrorism
- Transportation Accident- Impacts Property/Employee
- Vendor- Supply Chain Risk
- Workplace Violence



# Are all threats equal?

# PREDICT: RISK ASSESSMENT

## WHICH THREATS ARE WE VULNERABLE TO?





# IS A GRAY HIPPO A BLACK SWAN?



# ACTIVE SHOOTER



**WHAT ARE THE ODDS IT CAN HAPPEN  
AT YOUR PLACE OF WORK?**

**DO THE ODDS MATTER?**

**THE REAL QUESTION IS: COULD THE SAN  
BERNARDINO SHOOTINGS HAVE BEEN  
PREVENTED?**

# WORKPLACE VIOLENCE

2,000,000 'reported' cases of workplace violence each year

*OSHA*

*By the way.....*

2.1 million bullies and 2.7 million victims  
American schools.

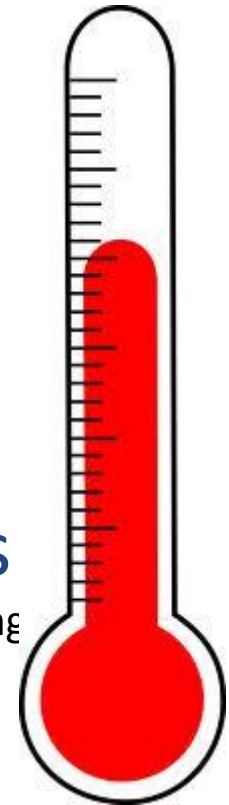
*National School Safety Center*

Death

Physical  
Injury

Threatening  
Behavior

Behaviors of  
Concern

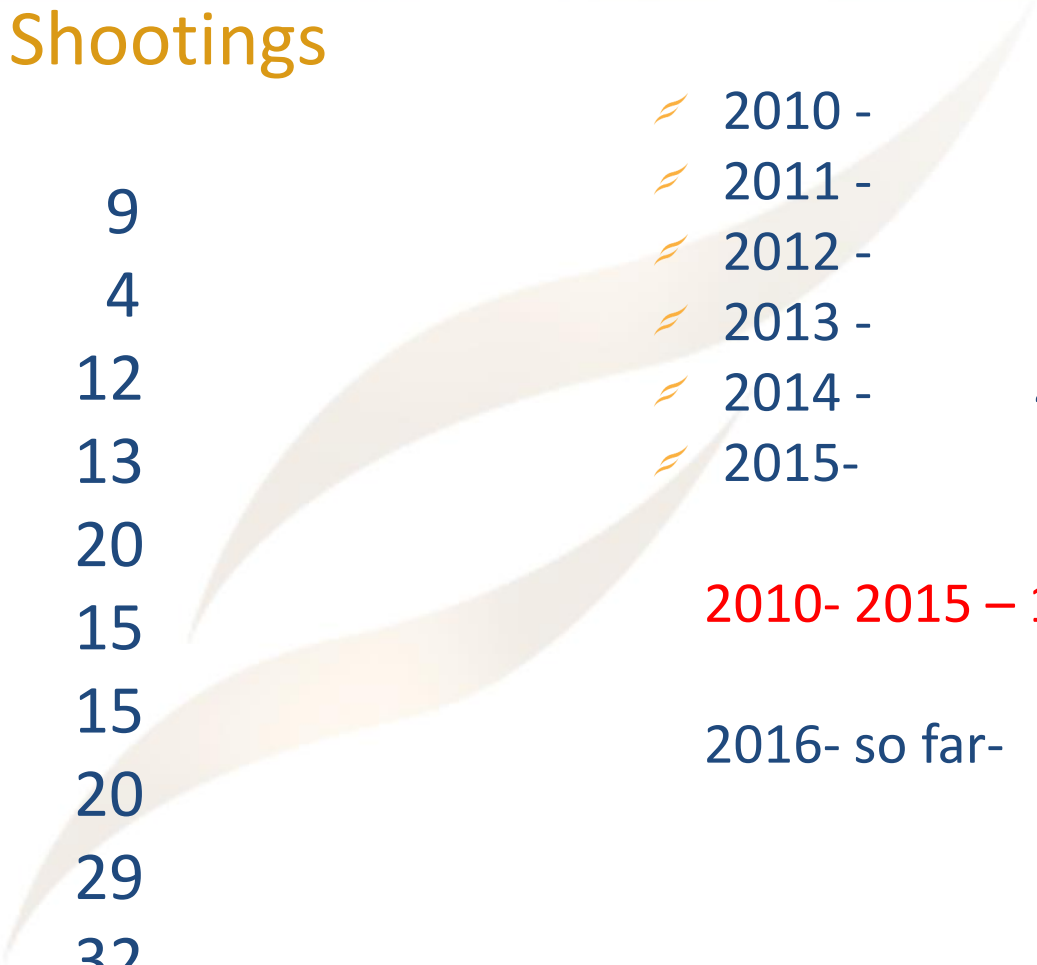


# HOMICIDE: LEADING CAUSE OF DEATH OF WOMEN IN THE WORKPLACE

- Leading cause- criminal intent- the second cause is abusive partners
- Over half of domestic violence incidents occur during normal business hours— broad daylight.
- The leading perpetrator of injuries to women in their professions is their patients.
- Women work in health care jobs that expose them to patients who may take a violent turn under loosely controlled conditions.— ***These incidents are preventable.***

# RATE OF CHANGE

## All School Shootings



✧ 1910s -	9
✧ 1920s -	4
✧ 1930s -	12
✧ 1940s -	13
✧ 1950s -	20
✧ 1960s -	15
✧ 1970s -	15
✧ 1980s -	20
✧ 1990s -	29
✧ 2000-09-	32

✧ 2010 -	8
✧ 2011 -	6
✧ 2012 -	9
✧ 2013 -	30
✧ 2014 -	40
✧ 2015-	20

**2010- 2015 – 113**

2016- so far- 6

Source: Wikipedia- List of School Shootings



# CYBER BREACH

- Today, 80% of the value of corporate assets has shifted from physical to virtual.
- 62% of all companies breached learned about the breach from customers
- 42% of the CISO's say they lack the budget and personnel to effectively detect and prevent breaches
- The chance of a cyber-security breach to your organization increases every day.
- Industries most Targeted:
  - Pharmaceutical
  - Financial
  - Healthcare
- If or when this happens, you will be impacted at many levels: *human, operational, reputational and financial.*



# MORE INFORMATION ABOUT BREACHES

- The Average Breach in U.S. involves 29,087 records
- Average Breach is undetected for **240 days**
- Average Breach Notification Costs \$509,237
- Average Lost Business Costs \$1,599,996
- Industries most Targeted:
  - Pharmaceutical
  - Financial
  - Healthcare

# GROWING CYBER EXPOSURE

- ✧ **Social Engineering** — Manipulation of people to perform actions or divulge information they otherwise would not perform or divulge
- ✧ **Crime**
  - ✧ Ensure that social engineering/fraudulent impersonation is added to your crime policy.
- ✧ **HIPAA**
  - ✧ Medical identity theft on the rise (value in Medicaid/Medicare numbers)
- ✧ **Cyber Liability**
  - ✧ Important to ensure that your cyber policy has coverage for social engineering
  - ✧ Identity theft coverage also typically found under this policy



# WHAT IS THE GREATEST THREAT ?



## The Rate of Change

*Technology is changing faster than anyone realizes. The rate of change is one of the biggest exposures the world faces today. Individuals, even those working in the technology field, are no longer able to forecast what the vulnerabilities and threats are of the technologies that are being created. Interestingly, Hollywood does a better job forecasting our exposures than people do.*

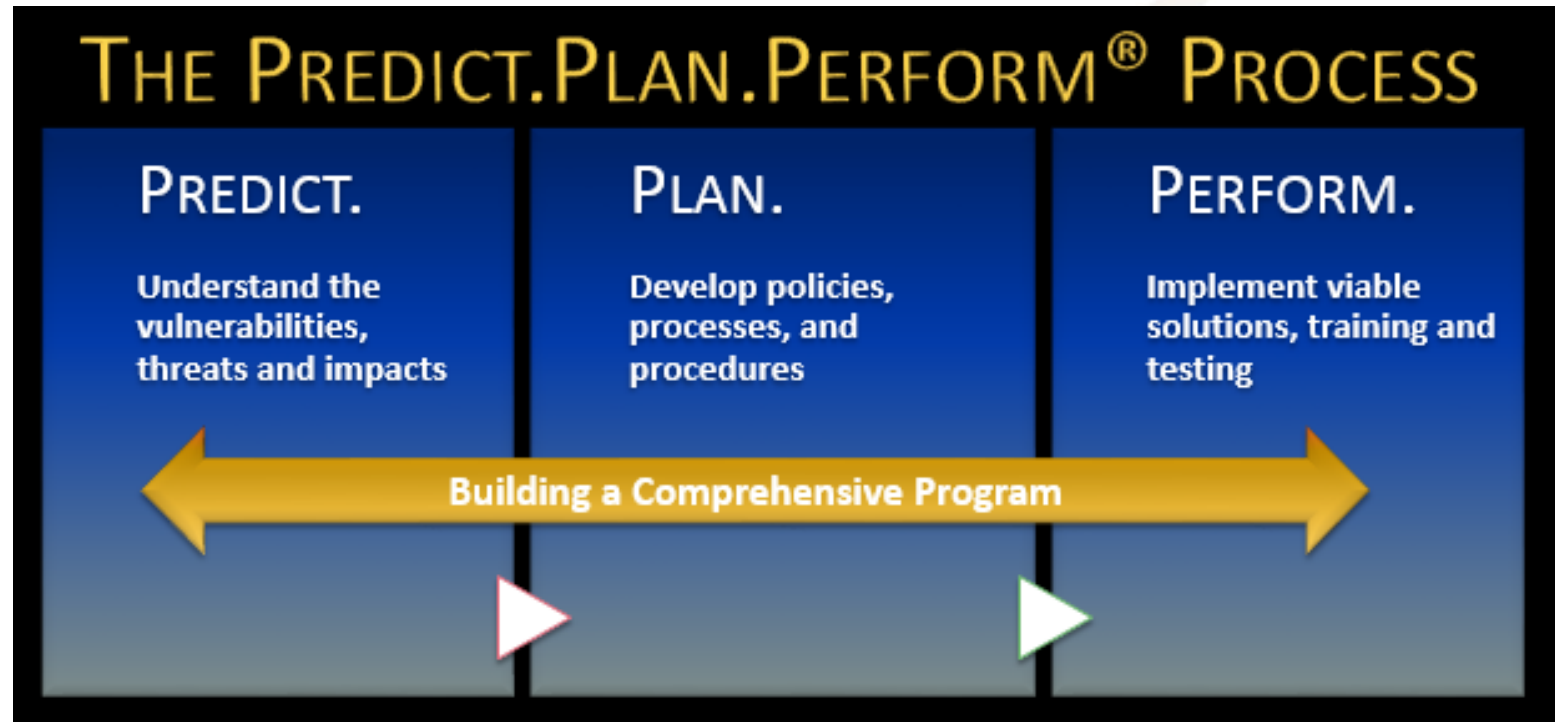
*~ Harry Rhulen, CEO Firestorm*

# IMPACTS & INSURANCE

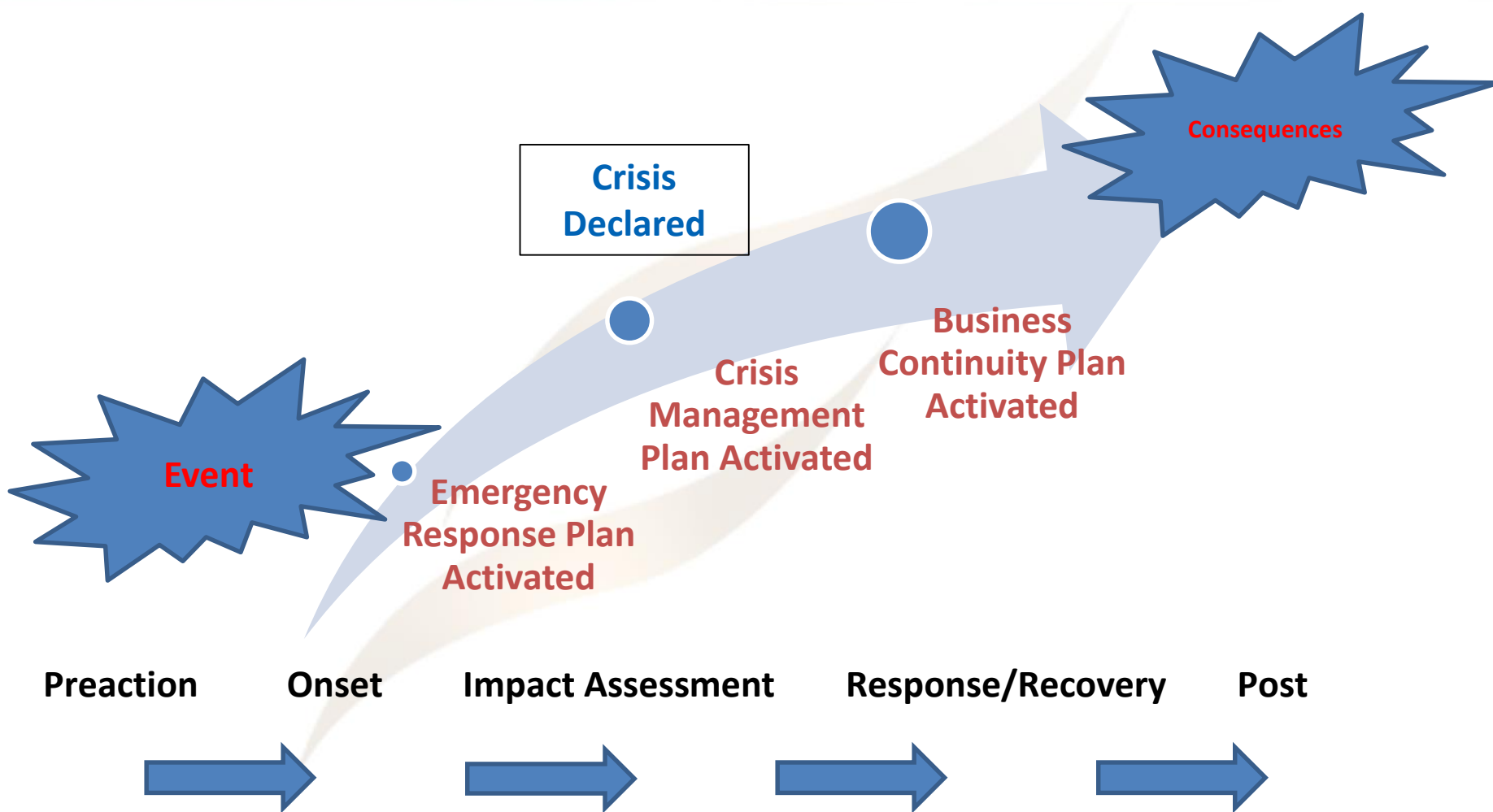
- Human (Injury/Fatalities)
- Financial (Property Damage, Business Interruption)
- Brand/Reputation
- Legal/Regulatory

# BUSINESS INCOME & EXTRA EXPENSE

- ✧ Business Income – net income you would have earned if a loss had not occurred
  - ✧ Standard 72 hour waiting period
- ✧ Extra Expense – Operating expenses incurred to continue normal operations
  - ✧ Save ALL receipts & proof of expenses
- ✧ Coverage triggered 4 ways
  - ✧ Direct Physical Loss
  - ✧ Off Premise Utility Failure
  - ✧ Civil Authority
  - ✧ Dependent Property



# TERMINOLOGY



# WHY PLAN?

- Increase **operational control** and efficiency in predicting, responding to, and controlling disruptions or crises.
- Promote and enforce a **culture of preparedness** that will protect company assets, employees, customers and reputation.
- Accelerate **return to normal** operations.
- Demonstrate **best practices**.
- **Reduce risk** profile.
- Preserve **reputation**.

# ACCOUNTABILITY

**TODAY**

***EVERYTHING IS  
FORESEEABLE***

**TOMORROW**

***ANYONE MAY BE FOUND  
ACCOUNTABLE***



## ✧ HIPAA

- ✧ Medical Identity theft
- ✧ Reputational harm

## ✧ Whistleblower (Qui Tam)

- ✧ Potential to close doors – critical to have processes to ensure appropriate billing

## ✧ FLSA

- ✧ Large financial exposure
  - ✧ Likely the cause of future re-organizing within the human services industry



# WHAT PLANS DO WE NEED?

- Emergency Response Plan
- Crisis Management & Crisis Communications
- Business Continuity
- Security Plan
- Workplace Violence
- Communicable Illness
- Cyber Breach Response

## EMERGENCY RESPONSE PLAN

### Plan Framework

- Tab 1 - Plan Overview
- Tab 2 - Crisis Response Overview
- Tab 3 - Emergency Communications
- Tab 4 - Roles & Responsibilities

### Threats/Hazards

- Tab 5 - Abuse
- Tab 6 - Armed Intruder
- Tab 7 - Bomb Threat
- Tab 8 - Electrical/Power Outage
- Tab 9 - Fire Emergency
- Tab 10 - Lost/Missing Camper
- Tab 11 - Medical Emergency/First Aid
- Tab 12 - Nuclear/Biological/Chemical
- Tab 13 - Offsite Emergency
- Tab 14 - Severe Weather
- Tab 15 - Visitor/Unwanted Guest Onsite
- Tab 16 - Waterfront Emergency

### Appendices

- Appendix A - External Contacts
- Appendix B - Request Call Scripts

## Contents

CRISIS COMMUNICATIONS PHONE NUMBERS .....	2
1. OVERVIEW .....	4
1.1 Purpose .....	4
1.2 Objective .....	4
1.3 Scope .....	4
1.4 Assumptions .....	5
1.5 Susquehanna Crisis Management Organizational Structure .....	5
2. AUTHORITY .....	5
2.1 Crisis Management Team Representatives .....	6
2.2 Computer Security Incident Response Team (CSIRT) .....	7
2.3 Incident Response Team Representatives .....	7
3. ROLES AND RESPONSIBILITIES .....	8
3.1 Corporate Crisis Management Team (CMT) .....	9
3.2 Subject Matter Expert (SME) Members .....	9
3.3 Computer Security Incident Response Team (CSIRT) .....	9
3.4 Incident Response Team (IRT) .....	10
3.5 Executive Advisor .....	10
3.6 Business Recovery Manager .....	10
3.7 Functional Recovery Teams .....	10
4. CORPORATE CRISIS MANAGEMENT TEAM ACTIVATION .....	11
4.1 Declaring a Crisis .....	11
4.2 Integrated Activation Structure .....	11
4.3 Notification Guidelines .....	12
4.4 Crisis Activation Matrix .....	13
4.5 Team Activation Guidelines .....	14
4.6 Corporate CMT Communication .....	14
5. CRISIS RESPONSE ACTIONS – CRISIS EVENT .....	15
6. CORPORATE CMT PHASES OF ACTIVATION .....	17
6.1 Corporate CMT Phase 1 – Prediction .....	17
6.2 Corporate CMT Phase 2 – Onset .....	19
6.3 Corporate CMT Phase 3 – Impact Assessment Phase .....	22
6.4 Corporate CMT Phase 4 – Response & Recovery Phase .....	23
6.5 Corporate CMT Phase 5 – Post Crisis Phase .....	26
7. INCIDENT RESPONSE TEAM (IRT) ACTIONS .....	28
7.1 IRT Phase 1 – Prediction .....	28
7.2 IRT Phase 2 – Onset .....	29
7.3 IRT Phase 3 – Impact Assessment .....	32
7.4 IRT Phase 4 – Response and Recovery .....	34
7.5 IRT Phase 5 – Post Crisis .....	36
8. CMT CRISIS SUPPORT .....	37
8.1 Corporate Communications .....	37
8.2 Facilities .....	39
8.3 Finance .....	42
8.4 Human Resources .....	44
8.5 Information Technology .....	47
8.6 Legal .....	49

## PLAN DETAILS MATTER

- In order to be most effective, plans need be concise, easy to follow, and most importantly, actionable.
- Plan language must be specific. Document the ‘how to do’, not just the ‘what to do.’

# EMERGENCY RESPONSE PLAN

## Two audiences to address when planning for an emergency:

- **All the Occupants in the Facility.** Employees require training on response protocols that guide their actions in the face of a threat of violence, (e.g. lockdown, flee/hide/fight).
- **Internal Emergency Response Personnel** (Emergency Response Team, Floor Wardens, Searchers, and Disability Aides): These are the internal personnel who are responsible for coordinating the response. They require an Emergency Response Plan that will:
  - Document ***roles and responsibilities***
  - ***Identify internal medical responders*** for first aid and CPR and incorporate emergency medical response protocols
  - Develop ***response procedures for evacuation, shelter-in-place, lockdown, and lockout***
  - Document ***response actions for scenarios*** such as bomb threat, armed intruder, etc.
  - Determine ***notification methodologies/tools*** and document their use in an emergency.

**Evacuate, Shelter, Lockdown, Lockout**  
**Flee/Hide/Fight**

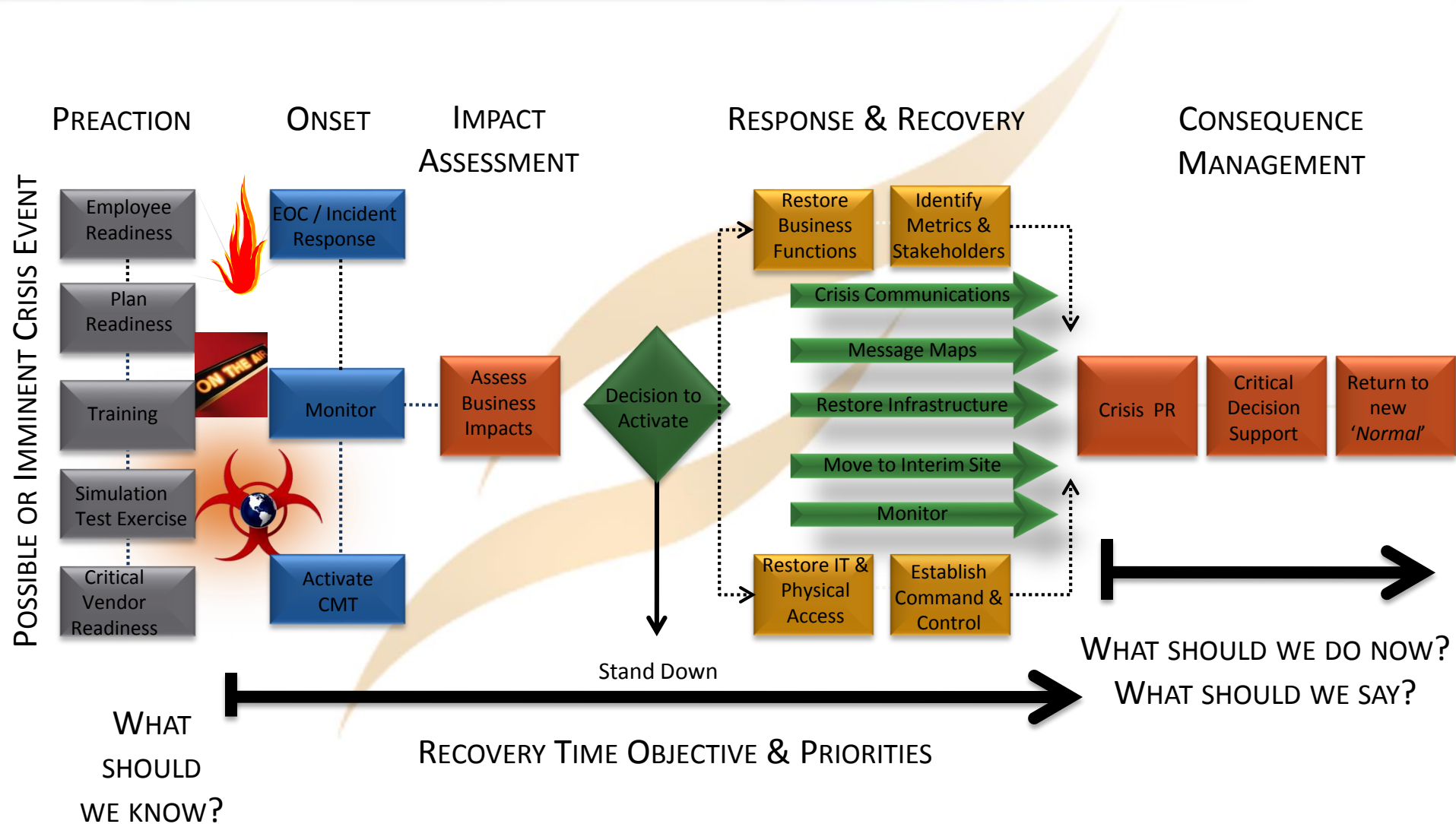
*“Do I stay or do I go?”*

# CRISIS MANAGEMENT PLAN

The purpose of this Crisis Management Plan (CMP) is to enable organizational leadership to respond, communicate, and manage crises in the most efficient and effective way possible regardless of the circumstances.

- Identify Crisis Management Team(s)- *they make the decisions!*
- Document communication protocols among groups- *Who is authorized to speak? Who is not?*
- Clarify roles and responsibilities- *Who does what?*
- Identify Stakeholders

# CRISIS MANAGEMENT PLAN



# SOME THREATS REQUIRE SPECIFIC PLANS

- ✧ Workplace Violence
- ✧ Cyber Breach
- ✧ Communicable Illness
- ✧ Hurricane

# WORKPLACE VIOLENCE PLANNING

**A Workplace Violence planning is about prevention.**

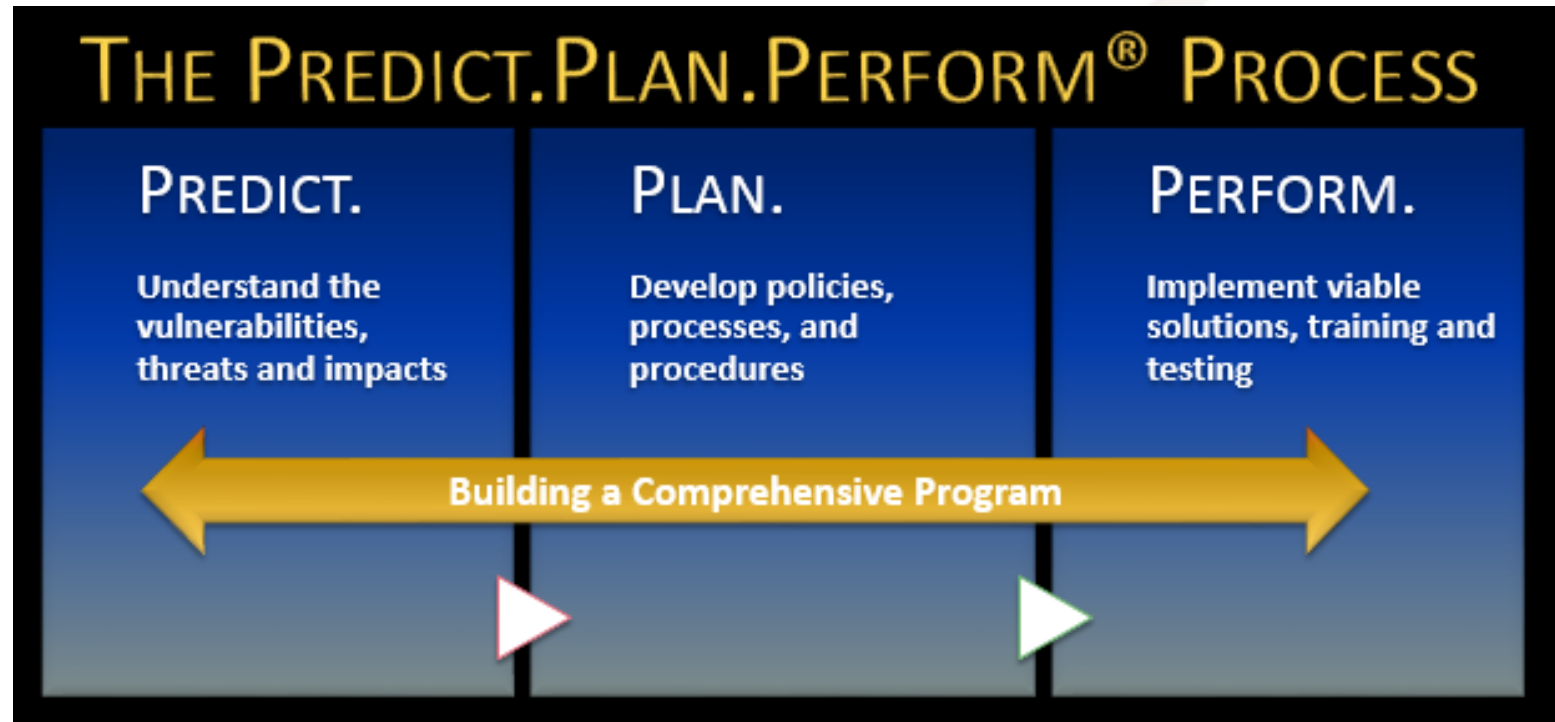
## **Four core dimensions:**

- **Behavioral Risk Threat Assessment (*BERTHA*™) Framework and Plan** – Assists in identifying, reporting, assessing, and managing individuals who exhibit warning signs and behaviors of concern.
- **Related HR Policies and Procedures** – Workplace violence, hostile workplace, bullying, and weapons policies, combined with appropriate disciplinary and termination procedures, help mitigate violence.
- **Emergency Response Protocols and Plan** – Guide employees and internal Emergency Response Teams in their actions in the face of a threat of violence, (e.g. lockdown, flee/hide/fight).
- **Security Planning** – Effective security is a combination of good facility management, information technology, and the latest security best practices.



# HOW DO WE REDUCE THE RISK OF VIOLENCE?

- Have Up-to Date Policies and Procedures (Weapons, Hostile Workplace, Bullying)
- Train **everyone** to know the warning signs and behaviors of concern that should be reported
- Security Features- Deterrence
- Develop a workplace culture where everyone is treated with dignity and respect
- Understand Behavioral Risk and Threat Assessment



# HAVE MESSAGING IN PLACE

**“Don’t let your first response become  
the second crisis.”**

*Harry Rhulen, CEO Firestorm*

# MANAGING A CRISIS TODAY IS VERY DIFFERENT....

## Good News:

- Don't need the press to tell your story
- You have the ability to talk to your stakeholders directly

## Bad News:

- Citizen journalists- no rules, no filter
- Capacity to build audiences quickly
- Video, text- in front of world instantly
- Speed of transmission- no time to 'respond'
- News = entertainment
- Constituents can be reached via social media by the press
- You are never 'off'- blurring of business & personal

# BE READY TO COMMUNICATE: EXPLAINING IS LOSING

Effective communication requires your organization to have established 'home bases' and pre-scripted message maps – approved in advance.

## HOME BASE # 1: WE WILL NOT BE DEFINED BY THE EVENT (WHAT DOES DEFINE YOUR ORGANIZATION?)

- *We are proud of our 40 year history of improving the lives of people with autism.*
- *We have earned a national reputation for excellence in serving people across the autism spectrum.*

## HOME BASE # 2: WE WILL INVENT THE FUTURE (WHAT IS YOUR ORGANIZATION DOING TO MAKE SURE THIS CAN NEVER HAPPEN AGAIN?)

- *We take the safety of all our students very seriously.*
- *We are constantly looking for ways to enhance the safety of our school and the environment for our students..*

## HOME BASE # 3: WE WILL EMBRACE THE FAMILY (WHAT IS YOUR ORGANIZATION DOING FOR THOSE IMPACTED?)

- *We are available to you at any time to discuss any concerns or questions you may have about your child's welfare, your child's experience at school, or our current policies.*

# THIS IS A CRISIS- WHICH NEEDED REAL CRISIS COMMUNICATIONS

## Jerry Sandusky Arrested: Ex-Penn State Coach, Athletic Director Tim Curley Charged In Child Sex Case



## Will Penn State president survive the Sandusky scandal?

**By Susan Snyder, INQUIRER STAFF WRITER**

POSTED: November 07, 2011

With 16 years at the helm of Penn State, Graham B. Spanier is one of the most highly regarded and visible college presidents in the country, but can he survive what has become perhaps the biggest black eye in the flagship university's history?

National higher education experts interviewed Monday said he likely can, but suggested he erred in speaking out so quickly in support of two administrators charged in a grand jury probe for their handling of child sex abuse allegations against former assistant football coach Jerry Sandusky.

On Sunday morning, Spanier in a statement announced his unconditional support of Senior Vice President Gary Schultz and Athletic Director Tim Curley, who have both been charged lying to a grand jury in the case.

"I have complete confidence in how they handled the allegations about a former university employee," Spanier said. Late that night, however, following a private meeting of the trustees, both men stepped down.



# WHO IS TO BLAME?







# KNOW WHEN TO COMMUNICATE

- Most organizations want to communicate immediately— even before they know the facts.
- They feel a need to be the ‘first’ source of information to their stakeholders.
- In today’s world, such communications are permanent— even if they contain wrong information.
- Any negative impact that comes from NOT being the FIRST source of information will be outweighed by being the ACCURATE source of information. You can apologize for delay. You can’t take back unnecessary and permanent damage you cause to your brand.

**WHEN YOU ARE EXPLAINING....  
YOU ARE LOSING !**

# PLANS MUST BE TESTED- OTHERWISE YOU WON'T KNOW IF YOUR PLAN WILL WORK

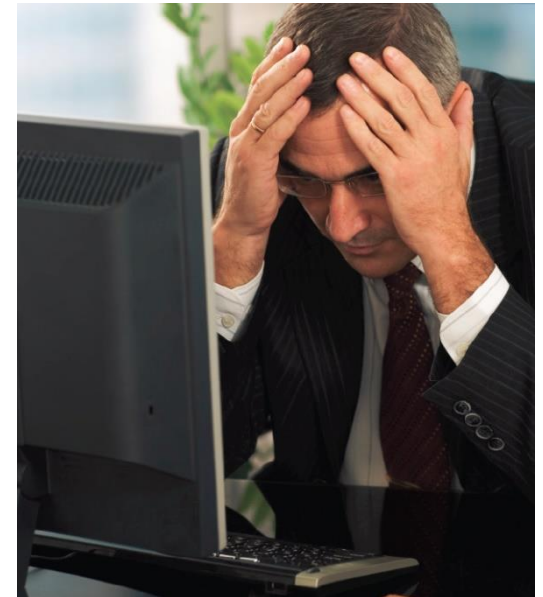


## Successful Crisis Management Hinges on:

- ✧ Establishing Command and Control- Appoint a General
- ✧ Identifying vulnerabilities, exposures & consequences
- ✧ Identifying all constituents you need to communicate with. *If you miss one, consequences could be catastrophic*
- ✧ Preparing messaging for all stakeholders
- ✧ Monitoring Merged Media
- ✧ Training spokespersons and everyone else on the media strategy

## Failure to have crisis control over a situation will result in:

- ✧ Damaging statements being made
- ✧ Exposures being missed
- ✧ Constituents being ignored
- ✧ Things falling through the cracks



# TIMING





# TIMING





If you had to respond now,  
are you ready?

PREDICT. PLAN. PERFORM. <sup>®</sup>

# FOR MORE INFORMATION



## CONTACT FIRESTORM:

Suzanne Rhulen Loughlin, Esq.

[sloughlin@firestorm.com](mailto:sloughlin@firestorm.com)

845 796 9811 Direct

845 313 0777 Cell

## CONTACT ISA:

Brad Storey, MSW

[brad.storey@siegelagency.com](mailto:brad.storey@siegelagency.com)

845 796 3400 Direct