Crisis Management—Are you prepared?

Denise Pacofsky, Partner, Deloitte & Touche LLP
Marshall Billingslea, Director, Deloitte Financial Advisory Services LLP

February 23, 2016
Presenters

Denise Pacofsky
Partner I Deloitte Advisory
Deloitte & Touche LLP
- Over 20 years of experience, largely international
- Focus on Crisis Management to assist companies in preparing for, responding to, and recovering from crisis events; international IPOs; regulation and public policy; auditing multinationals

Marshall Billingslea
Director I Deloitte Advisory
Deloitte Financial Advisory Services LLP
- Supports Deloitte Advisory’s work with NATO, the European Union, US Special Operations, and Intelligence communities
- Prior to Deloitte Advisory, held senior positions within US Federal Government and overseas, including Deputy Under Secretary of the Navy, Assistant Secretary General of NATO for Defense Investment
Your poll will show here

1. Install the app from pollev.com/app
2. Make sure you are in Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser
Your poll will show here

1. Install the app from pollev.com/app
2. Make sure you are in Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser
Have you experienced a corporate crisis?

- Yes, it was horrific
- Yes, it was not so bad
- Yes, barely
- No

What was the most challenging aspect of the crisis?

- We were not prepared
- We were in denial
- Events unfolded so fast
- We overanalyzed
- Media was unforgiving
- Would have been different before the days of social media
- All of the above
- Other
- N/A
THE FIVE STAGES OF A PR DISASTER

MAYBE IT WILL ALL BLOW OVER.

HOW DARE ANYONE CRITICIZE? WE'RE THE VICTIMS!

PLEASE LEAVE OUR FACEBOOK WALL OUT OF IT.

WHAT WILL THIS DO TO OUR BRAND?

WE ACCEPT THAT OUR LAWYERS WILL DRAFT A HEARTFELT NON-APOLOLOGY.

DENIAL

ANGER

BARGAINING

DEPRESSION

ACCEPTANCE

Source: marketoonist.com, February 5, 2012
Your poll will show here

1. Install the app from pollev.com/app
2. Make sure you are in Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser
Your poll will show here

1. Install the app from pollev.com/app
2. Make sure you are in Slide Show mode

Still not working? Get help at pollev.com/app/help
or
Open poll in your web browser
What is your biggest crisis concern today?

- Cyber attack
- Food safety
- Financial crime
- Labor disputes
- Natural disaster
- Terrorism
- All of the above
- Other
- Not sure

In your opinion, how equipped is your organization to handle a crisis?

- Ready to go – robust program in place
- Currently working to mature our capabilities
- Not very prepared
- Not sure
“A reputation crisis – where a company may suddenly lose more than a fifth of its value – carries an 80% likelihood in a five year period.”

Source: Oxford Metrica and Aon Reputation Review 2012
… a major catastrophic event, or a series of escalating events, that threatens an organization’s strategic objectives, reputation, or viability.

Crises typically exceed existing mitigation techniques and risk management programs such as Business Continuity, Disaster Recovery, Health and Safety plans, or Emergency Response.
Crises have grown in severity and frequency

- **$400B** annual cost to the global economy from records stolen due to cyber attacks
- **300+** natural disasters
- **500+** major boycotts, riots, and labor disputes globally
- **~$9B** total loss for man-made disasters
- **1.2K** corporate fraud and embezzlement cases in US

Source: See Appendix slide for sources
Hospitality industry has similarly experienced a wide spectrum of crises, with increased frequency

The data below represents actual events that placed a hospitality company in the public spotlight and often resulted in financial implications.

Social media can quickly instigate a slow burn. Twitter has 320 million users who post 500 million tweets per day.

Timeline is illustrative, not drawn to scale, and represents crises noted from public sources.

Source: Deloitte analysis, Twitter September 30, 2015
Crisis management capabilities are integral to an organization’s ability to manage unforeseen crises.
## Moving toward effective crisis management

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Organization</td>
<td>Pre-defined group of senior leaders responsible for all aspects of organization’s response</td>
</tr>
<tr>
<td>Crisis Management Plan</td>
<td>Guidelines and procedures developed in advance of a crisis</td>
</tr>
<tr>
<td>Common Operating Picture</td>
<td>Situational awareness capability</td>
</tr>
<tr>
<td>Decision Making Process</td>
<td>Structured approach for analyzing situation, identifying issues, assessing options, taking decisive actions</td>
</tr>
<tr>
<td>Control Hierarchy</td>
<td>Structure that defines decision rights, leadership succession, other management controls</td>
</tr>
<tr>
<td>Crisis Communications</td>
<td>Communications internally and externally during a crisis</td>
</tr>
<tr>
<td>Information Management</td>
<td>Formal documentation to track the details of the event and response actions</td>
</tr>
<tr>
<td>Ongoing Crisis Monitoring</td>
<td>Collecting and analyzing pertinent information on a continuous basis throughout the crisis</td>
</tr>
<tr>
<td>Private — Public Coordination</td>
<td>Integration between public and private sector to respond to events that may involve critical infrastructure and key resources</td>
</tr>
</tbody>
</table>
Effective crisis response is essential to preserving shareholder value

Crisis challenges can delay and degrade response

Crisis Characteristics

- Sudden, unexpected event or multiple precipitating events
- Compressed time for decision-making and action
- High potential for negative impact to organization
- High uncertainty, low clarity
- High media scrutiny
- Significant business disruption

Effective crisis response shown to reverse negative effects on shareholder returns

Source: Research from 15 high-profile crises focused on the impact on shareholder value following the crisis; Oxford Metrica and Aon Reputation Review 2012
Your poll will show here

1. Install the app from pollev.com/app
2. Make sure you are in Slide Show mode

Still not working? Get help at pollev.com/app/help or Open poll in your web browser
Your poll will show here

1
Install the app from pollev.com/app

2
Make sure you are in Slide Show mode

Still not working? Get help at pollev.com/app/help or Open poll in your web browser
### Who is on point to lead a crisis for your organization?

- CEO
- CFO
- Chief Risk Officer
- Legal
- PR/Communications
- SME (i.e., CIO for cyber)
- Other
- Unsure

### In your opinion, who might be the most overlooked stakeholder in a crisis?

- Customers
- Employees
- Investors
- Media
- Third parties/vendors
- Other
- Not sure
Is your organization prepared to be in the spotlight?

- **Does this impact our bank covenants?**
- **By how much will we miss our earnings estimate?**
- **What’s the damage to our business?**
- **What’s our legal exposure?**
- **What really happened?**
- **Which controls and procedures were violated?**
- **Is our credit rating vulnerable?**
- **How much cash will we bleed?**
- **What’s the damage to our business?**
- **How will reputation loss impact the company’s long-term viability?**
- **Who’s to blame?**
- **Can we trust you to keep your financial commitments?**
- **How safe are our jobs?**
- **What penalties and fines are we exposed to?**
- **How will reputation loss impact the company’s long-term viability?**
- **Who’s to blame?**
- **Can we trust you to keep your financial commitments?**
- **How safe are our jobs?**
- **What penalties and fines are we exposed to?**
Rehearsing and practicing *before* a crisis can lead to greater success with crisis response and recovery.

**Table-top Exercises**
- Training-based
- Informative
- Consensus building
- Walkthrough scenarios, passive environment

**Simulations**
- Practice roles and processes/explore strategies
- Examine assumptions
- Increased pressure and focus on timely decision making
- Scripted, active environment
- Hot-wash debrief

**War Games**
- Stress test assumptions
- Worst-case scenarios
- Red team–adversarial group playing against participants
- Free play, interactive environment with open debates
- Hot-wash debrief
- After action report
War Games can enable risk-informed decision-making through immersive and experiential learning

Plausible scenarios are customized depending on requirements and can include exploring an issue, assessing capabilities against established processes, or anticipating future risk and examining an organization’s ability to manage it.

### War Game Types

- **Discovery**
  
  Illuminates emerging crises and risks, and their impacts; and identifies ideas to prepare, respond, and recover

- **Assessment**
  
  Evaluates current plans, procedures and capabilities; and identifies gaps for improvement

- **Strategic Futures**
  
  Probes future environments to recognize emerging threats, enabling pro-action rather than reaction

### War Game Outcomes

- **Improved Understanding**
  
  Breaks through organizational bias and enables common understanding of risks

- **Identification of Alternatives**
  
  Enables development and refinement of alternatives and their effects

- **Readiness and Reduced Surprise**
  
  Enables organizations to be better prepared through rehearsing in a simulated environment

“I hear and I forget, I see and I remember, I do and I learn.” - Confucius
Overview—hotel terrorism

An increase of hotel terrorist attacks prompts a reevaluation of current security postures within the hospitality industry. Adapting to this threat environment will require new approaches and the implementation of industry-wide security standards.

Indicators of attractiveness
Identify indicators that make hotels attractive targets
Understand vulnerable exposure points that can be exploited by terrorists

Trends in terrorism
Understand global terrorism trends and implications on hotel security.

Success factors
Outline critical factors needed to effectively adapt to the threat environment

Leading Practices
Highlight leading practices for implementing success factors
Attractiveness of a target

Terrorists are focused on targets that provide the greatest return on investment. Hotels often exhibit many of the qualities that make a target “attractive” to terrorists.

- Dense western populations
- Symbolic of western values, culture
- Traditionally weak security posture
- Requires few resources
- Involves minimal planning
- Potential to elicit fear among the masses
Increases in hotel terrorism

Trends in global terrorism appear to correlate with hotel terrorism and are on the rise. This should spur both owners and operators in the hospitality industry to reconsider hotel security strategies.

Casualties Per Terrorist Attack 2005-2015

Critical success factors

These critical success factors set forth a multifaceted strategy to help address the security vulnerabilities that make hotels attractive terrorist targets.

- **Background checks**: Comprehensive vetting process not only validates skills, but also helps protect against potential insider threats. Background checks should be performed on hotel employees, vendors, and contractors.

- **Well-trained employees**: Every hotel employee plays a role in maintaining the security of the property and its guests. Therefore, training in basic security awareness and response should be a necessary component of every employee’s orientation and continued training.

- **Multi-layered security**: The application of proactive, effective security capabilities include layering security--crucial for protecting hotels and guests from terrorist attacks.

- **Community buy-In & engagement**: Approximately 98 percent of terrorist attacks live within 28 miles of their target.* The more that a hotel is locally connected, the more likely it can keep abreast of patterns of behavior in the community that may signal preparation activities for an attack.

- **Symbolic appeal**: By understanding what makes a soft target appetizing to a terrorist group, countermeasures may be taken to minimize the profile of the hotel.

- **Industry standards**: There is a need for coordination across the hospitality industry to establish a global security framework with minimum standards and leading practices.

* Data Source: National Institutes of Justice
Leading practices

While there is no proverbial silver bullet, the current and emerging trend of hotel terrorist attacks requires an integrated response anchored in leading practices.

**Security Assessments**
Perform routine hotel security assessments to identify security gaps and vulnerabilities.

**Security Strategy**
Develop a security strategy that enables the business capabilities, services, and processes to function with minimal disruption.

**Regular Meetings**
Conduct regular employee meetings to develop a shared understanding around critical functions of hotel security.

**Communications**
Employ strategic communications to sustain buy-in from community leaders and encourage employees to keep hotel security staff informed.

**Policy Guidance**
Provide clear policy guidance for the establishment of a security strategy that defines roles and responsibilities throughout the hotel compound.

Fully integrating robust security measures and leading practices into daily operations is essential to preserving security.
Summary

The identified critical success factors and leading practices can serve as a model for standing up a capability for hotels to mitigate the risk and reduce the impact of a terrorist attack.

Implemented together, hotels have the ability to improve security effectiveness. This mission is essential to preserving the confidence of travelers.
Questions
Feeling ready vs. being ready – board survey results

Board members feel ready to handle crisis, but a deeper dive hints otherwise

How would you rate your organization’s crisis management strategies and capabilities?

- 62% Overall
- 82% Over US$10B revenue

Respondents who answered "4" or "5" on a five-point scale where 1= not at all prepared and 5= fully prepared

Fewer than half of the total respondents say they have a “playbook” that sets out some of the options, actions and decisions that may be required for specific, defined crisis scenarios.

Does this organization define a specific set of actions—a distinct “playbook”—for each of its specifically defined crises scenarios?

- Yes: 49%
- No: 18%
- Uncertain: 33%
Most steps toward crisis preparedness go ignored

Half the total respondents or fewer reported having engaged in each of a list of specific crisis preparedness activities.

- Evaluated key crisis scenarios: 50%
- Evaluated strengths/weaknesses/opportunities/threats (SWOT): 50%
- Identified relevant stakeholders: 49%
- Engaged multifunctional teams: 46%
- Evaluated worst-case scenarios: 43%
- Evaluated stakeholders in analysis of specific scenarios: 41%
Ranking the threats – board survey results

We asked companies how vulnerable they might be to the following potential crises (on a scale from 1-5 where 1 = not at all vulnerable and 5 = extremely vulnerable)

Across all industries, locations, and company sizes, the most commonly cited vulnerabilities were corporate reputation and cyber-crime. Chemical, biological, radiological, or nuclear attack and the threat of workplace violence were at the bottom of the list.
(If answered Yes to 2A or 3) Having indicated earlier that you have gone through a crisis—what are the lessons that your company has learned, or that you would do differently? Choose top three

- Do more to better identify potential crisis scenarios: 34%
- Invest more effort in prevention: 27%
- Improve detection and early warning systems: 32%
- Monitor social media as a means of detection: 16%
- Better define the chain of command for specific scenarios/situations (roles/responsibilities/timing): 23%
- Conduct better pre-crisis planning for coordinating communication with emergency responders and government agencies: 28%
- Execute a more timely and robust communications plan: 29%
- Communicate more effectively with business partners/alliances: 28%
- Communicate more effectively with employees: 29%
- Communicate more effectively with customers: 28%
- Communicate more effectively with suppliers: 24%
- Other: 2%
Many organizations face challenges and stumbling blocks that can delay or degrade crisis response

- Excessive focus on fixing the incident, rather than leading the response and addressing the strategic impacts
- Failing to understand or underestimating the scale, breadth, and speed of the crisis and its unanticipated consequences
- Making inaccurate decisions and unintentionally causing harm, due to bad or incorrect information in the first few hours of a crisis
- Not having enough time to make sense of the chaotic inflow of information and answering all of the direct inquiries
And furthermore, in a crisis…..

- Have a plan in place and exercise it before a crisis hits
- Lead decisively – remember, taking no action is making a decision
- Continually frame the crisis – don’t underestimate the scale, breadth, and speed of the crisis and its unanticipated consequences
- Focus on what you can control; accept what you cannot
- Address the strategic impacts – avoid excessive focus on fixing the incident
- Avoid analysis paralysis – you will never have all the information
- Actively communicate – own the story, don’t let others tell it for you
- Be ready for the unexpected
- Drive toward actionable intelligence
- …Don’t panic
For further information

Denise Pacofsky
Partner | Deloitte Advisory
Deloitte & Touche LLP
dpacofsky@deloitte.com

Marshall Billingslea
Director | Deloitte Advisory
Deloitte Financial Advisory Services LLP
mbillingslea@deloitte.com
Appendix
Sources for slide: ‘crises have grown in severity and frequency’

Sources:


Other catastrophes: Swiss Re: Natural disasters and man-made disasters 2011

Sources of data points on the right:

800 Billion individual records lost with an annual cost to the global economy of more than $400 Billion: Net Losses: Estimating the Global Cost of Cybercrime June 2014 – McAfee