Riding Out the Storm: How to Weather a Crisis and Mitigate Future Problems

May 21, 2014
Panelists

> Moderator: Jamey Tesler – Of Counsel, Greenberg Traurig, Government Law & Policy

> Julia Coyne – Assistant General Counsel, Nike

> Elizabeth Fraser – Shareholder, Greenberg Traurig, Corporate & Securities

> Jeffrey Greene – Shareholder, Greenberg Traurig, Litigation

> Christine Nickerson – Director of Labor Law, Ahold USA
“There cannot be a crisis next week. My schedule is already full.”
- Henry Kissinger
Setting the Stage

> Crisis is unavoidable
> Increasing array of potential crises
  – Government investigations
  – Global product recalls
  – Infrastructure or security threats
  – Financial restatements
  – Shareholder activism
  – Labor disputes
  – Employment/Personnel problems
> Disastrous effects if not handled well
“Bad companies are destroyed by crisis. Good companies survive them. Great companies are improved by them.”

- Andy Grove (former CEO of Intel)
Key Components of Crisis Management

- Plan for crisis
- Practice for the known and unknown
- Identify the team (beforehand)
- Document (electronic) control
- Pro-active approach
- Communication internally & externally
- Don’t ignore or defend the problem – Fix it!
- Post-crisis debrief/evaluation process
Planning for Crisis

> Strong foundation
> Maintain up-to-date best practice policies, procedures, internal control plans
> Disaster Recovery Plan/Continuing Operation Plans
> Top management/board/committee to identify predictable events
> What about the unknowns? What about the “that will never happen to us” scenario?
> Crisis communication center
> Internal system for communication
Practice for the Known and the Unknown

> Disaster Recovery Plans/COOPs require frequent practice

> Who should participate in practice drills?

> Focus on the details

  – Contact list

  – Where is the hard copy of the plan stored?

  – Remote location

  – Prepare your command center and senior leadership for when offices and the network is down
Identifying the Team

> Team members typically include:
  > – Member of management
  > – Legal
  > – Operation/IT
  > – Public/Investor relations
  > – HR and possible Business Unit Level Management
  > – Outside advisers

> Know your “first responders”

> Involvement of Board/Committee

> Involve PR firm early

> Prepare an action plan for the first 24 hours
Get Control of Documents, Especially Electronic

> Understand what documents/data need to be protected/preserved/collected – fast
  – Find your IT champions (in advance) to help

> Understand your data risk points – IP, PHI, PII, proprietary business data – and develop risk classifications
  – Establish security policies for critical data sources
  – Train your employees on how to handle sensitive data

> If litigation is pending or threatened, issue timely written legal hold notices to preserve relevant data
Get Control of Documents, Especially Electronic

> Is issue data critical - is key data rolling off the table as we speak? Should data be locked down to avoid spoliation?

> Know your limitations – where data is critical, utilize expert/vendor to extract/preserve data

> When conducting your investigation and securing your data, utilize repeatable, defensible processes

  – Avoid jumping to conclusions

  – Avoid shortcuts in process – unless they can be justified and detailed

  – Document your processes for defensibility purposes
Leadership

> Successful management requires a team leader
> Positive and engaged management and Board
> Tone at the top matters for customers and employees
The Apology

> Act fast
> Say “I’m/We’re sorry”
> Acknowledge the problem
> Explain why problem does not reflect mission/values of company
> Explain how it will be fixed/has been fixed
> Describe how the company will learn from it
> Be sincere
GC’s Role as Coordinator/Leader

> May need to be central point of contact

> Attorney/Client considerations
  
  – Ability to act as communicator among team members

  – Communicate with Board, outside advisers, PR firm, insurance carrier

> Responsible for records preservation/storage/ID
Speed Matters

> Don’t get behind

> Stay pro-active

> Don’t let your customers, clients, regulators wait too long for answers

> Good preparation, planning and practice pay off

> Implement your plans, don’t react
Communications

> Identify your spokesperson
  – Needs to have good communication skills, calm under pressure, experienced with communicating to the public
  – Know who this person is BEFORE the crisis

> Identify who needs to know what and when
  – Don’t let employees clog the communication channels
  – Make sure essential communications get through

> Clear, consistent communications to all impacted
  – Employees
  – Customers
  – Suppliers
  – Investors
Communications (continued)

> Social media
  - Damaging information spreads virally, regardless of accuracy
  - Cannot ignore the importance of good PR/social media response to any crisis

> Know your required communications (regulators)

> Be mindful of environmental, health and safety issues

> Resist any defensiveness
  - Find problems
  - Acknowledge problems
  - Identify improvements
After the Crisis

- Objective evaluation is key
- Debrief with management/board/committees
- Develop recommendations on how to improve and implement crisis management strategy
- Anticipate next problem
- Engage in regular review, assessment and testing of your crisis management plan
Questions?