Facing the Unknown:
Crisis Management and the Role of Internal Audit

April 11, 2016
A crisis is...

“... a major catastrophic event, or a series of escalating events, that jeopardize the critical assets, reputation, and financial standing of an organization or community.”

Crises typically exceed existing mitigation techniques and risk management programs such as Business Continuity, Disaster Recovery, Health and Safety plans, or Emergency Response.
Types of crisis events and triggers

**Natural or man-made destructive events that disrupt almost everything**

The explosion of a power plant due to a hurricane, led to massive electricity outages. The ensuing investigations revealed poor governance and oversight leading to a fall of nearly $2B in market value for the utility.

**Complex systems fail, either through accident, mismanagement or sabotage**

A massive explosion at a chemical plant caused loss of property and infrastructure of over $100M, and injuring nearly 200 people. It was later discovered that a small fire had spread to a highly combustible stockpile causing the explosion.

**Fraud or other criminal activity**

A leading drug manufacturer was fined around $3B for bribing and giving kickbacks to doctors for prescribing unsuitable medicines.

---

**Legal, commercial, geopolitical, or military conflicts**

A healthcare giant faced a massive disruption when more than 2000 employees went on strike to protest against its failure to provide patients with access to health services. The company had to face investigations, regulatory scrutiny, and pay nearly $5M in fines.

**Deliberate acts such as identity theft, product tampering, cyber-attacks, or cyber-crime**

A bank had significant reputational impact after an unprecedented data breach compromised over a 100 million accounts of households and small businesses. On investigation, it was revealed that the breach (unnoticed for over a month) could have been avoided by a simple security fix.

**Unforeseen failures that threaten a company’s very existence**

A prominent gaming company in the U.S. filed for Chapter 11 bankruptcy protection after failing to meet its covenants on nearly a $50M debt facility. The company had been posting huge financial losses for multiple years, mainly due to poor sales and failure of products in the market.
### Crisis examples

Looking back at crisis events in the U.S.

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Details</th>
</tr>
</thead>
</table>
| **HURRICANE KATRINA - New Orleans, Louisiana** |                           | 1. Category 3 Hurricane Makes Landing in 2003  
2. Billions of Dollars of Damage Caused In The City  
3. 2,000 Resident Deaths  
4. 100,000 Homes Destroyed |
| **GENERAL MOTORS – Faulty Parts**         |                           | 1. Defective Ignition Switches Placed in GM Cars  
2. Linked to 124 Deaths  
3. Linked to 275 Injuries  
4. 2.6 Million Vehicles Recalled |
| **CHIPOTLE MEXICAN GRILL - E. Coli Poisoning** |                           | 1. 200 People Become Sick in August of 2015  
2. Chipotle Forced To Temporarily Close Doors  
3. Chipotle Stocks Fall Following News |
| **TARGET – Data Breach**                  |                           | 1. The breach cost Target $148 million in just 2014  
2. Target spent nearly $200 million in 2014 to upgrade systems  
3. Over 70 million had personal information compromised  
4. Target’s stock price recovered in 2014 but sales declined by more than 2% |

In 2014, GM had multiple recalls as faulty engineering was exposed. The stock price declined from $37.86 in February 2014 to $29.48 in February 2015.

Chipotle’s stock value experienced year over year increases but in the last 12 months, the stock has declined nearly 2%.
The dynamic VUCA\(^1\) business environment has led to larger and more frequent crisis events globally.

**World has seen a drastic increase in crisis incidents...**

**Leading to massive loss of market value across industries...**

An internal Deloitte study\(^3\) shows that 86 top crisis incidents during 2012-13 have resulted in a cumulative market value loss of $351B, and other financial losses of $45B.

### Annual Worldwide Catastrophes\(^2\)

- **Number of events**
  - 50
  - 75
  - 100
  - 150
  - 200
  - 250
  - 300
  - 350
  - 400
  - 450

- **Market cap. losses in $ bn**
  - 10.8
  - 1.6
  - 56.6
  - 88.4
  - 115.5
  - 77.6

### Triggers of Crisis

**Financial disruption**
- More than 47,000 bankruptcies in US alone

**Malevolence & cyber**
- More than 4,000 successful cyber-terrorism attacks globally

**Confrontations**
- 500-600 major boycotts, labor disputes and riots globally

**Technological & industrial**
- Nearly 50 major industrial disasters globally

**Misdeeds & financial crime**
- Nearly 700 corporate fraud and 500 embezzlement cases in US

**Other catastrophes**
- More than 300 catastrophes globally

---

1. VUCA – short for volatility, uncertainty, complexity, ambiguity
2. Swiss Re: Sigma world insurance database
3. Source: Crisis management: Analysis of crisis impacted companies
4. Source: Combination of sources detailed in speaker notes
Organizations are faced with various challenges when addressing novel crises

Leaders often have to take charge and rally their troops to avoid some common stumbling blocks such as:

- 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 poor 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
Responding to a crisis requires a broader organization-wide view and a multi-pronged approach.

Crisis Management Program

Response Organization  Crisis Management Plan  Common Operating Picture  Information Management  Crisis Communications  Private-Public Coordination  Control Hierarchy  Decision Making Process  Ongoing Crisis Monitoring

Routine crises are typically addressed through Business Continuity and other plans within departmental silos.

Business Continuity  Emergency Response  IT Disaster Recovery  Environmental Safety  IT Security  Facilities  Communication s / Public Relations  Travel Security  Insurance  Others...

Crisis Triggers

Critical Infrastructure  Intellectual Property (IP)  Reputation and Brand  Financial Data
In order to stay ahead of growing threats and the dynamic nature of crises events, organizations must invest in identifying, preparing for, and responding to the strategic risks:

- Strategic Risk / ERM Assessment
- Crisis Management Planning
- Scenario Planning
- Wargaming & Simulation
- Crisis Communications
- Real Time Response
- Post-crisis Response
- Post-crisis Recovery
- 24/7 Monitoring

**Types of crisis events include, but are not limited to:**

- Technological & industrial, including recalls
- Malevolence & cyber attacks
- Misdeeds & financial crime, including fraud
- Financial disruption and bankruptcy
- Confrontations – Legal, commercial, geopolitical, or military conflicts
- Natural disasters and other catastrophes
The role of internal audit

The IIA definition of internal audit lends itself to a natural role in crisis management

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
Assurance and Consulting roles for internal audit in Crisis Management
Internal auditors can help provide an organized approach to prepare for, and deal with a crisis via a comprehensive Crisis Management Program

- Carefully select the crisis management team members and make sure they have the requisite skills and experience to perform the roles they may be expected to assume in a crisis.
- Continuously monitor the internal and external environment, leveraging technology, to adapt your response to the crisis.
- Establish documentation (forms and process) to track the details of the event and response actions throughout the crisis.
- Establish the means to collect, analyze, and disseminate situational awareness to the stakeholders that need to be informed and/or take action.
- Lead coordination between outside public and private sector entities to respond to events that may involve critical infrastructure and key resources.
- Develop and maintain a clear and concise set of guidelines and procedures to identify the actions, issues, and responsibilities that need to be addressed before, during, and after the crisis.
- Define a clear structure and order around decision rights, leadership succession, and other management controls.
- Maintain a structured approach for analyzing the situation, identifying issues, assessing options, and taking actions.
- Implement a comprehensive communication plan driven by executives. Tone and leadership need to be “set from the top”.

Copyright © 2016 Deloitte Development LLC. All rights reserved.
Resilience program

A Resilience program enables an organization to navigate a disruption, it also enables the Board of Directors and executives to confidently maintain their accountability to stakeholders in the event of a crisis. Programs that demonstrate four characteristics generate the greatest value to all stakeholders.

- Relevant to executives
- Beneficial to a broad set of stakeholders
- Quantifying risk and mitigation effectiveness that justifies investments
- Metrics and reporting that enable executives to make informed funding decisions about business continuity
Tips to successfully engage the organization in crisis management

**Tips**

**Engage executives and other senior leaders:**
A successful resilience program begins with buy-in and support from the top. As the first step, we recommend engaging cross-functional executives and other senior leaders to collaborate and agree upon:

- resilience policy
- governance structure including roles and responsibilities
- recovery tiers and impact (risk) tolerances
- crisis management team composition

**Use a simple design with the business stakeholder in mind:**
Resilience activities such as data gathering, planning, and exercising provide valuable touch points with the business and technology resources. If those touch points are complex, time-consuming, boring, and lecture-centric they won’t encourage future participation. Additionally:

- consider each business interaction as a time to engage with the business and use it as a selling point to show the value of the program.
- integrate into current day-to-day processes wherever possible for sustainability

---

*Governance and Operating Model*

**Roles & Responsibilities**
...establishing accountability and expectations

**Methodologies**
...for effective/consistent playbook, development, testing, risk assessments, & more

**Goal & Vision**
...establishing the direction of the Program and key performance metrics

**Program Policy**
...leadership’s message to the organization and commitment to the program

**Resources**
...internal FTE’s and/or external advisors to develop and maintain the program

---

Copyright © 2016 Deloitte Development LLC. All rights reserved.
Tips for successful planning

**Understanding of Processes**
Understanding the various processes that exist within a business unit is critical before recovery strategies and procedures can be written. It is best practice to learn about the business unit prior to beginning any development workshops—this also helps gain credibility with participants.

**The Right People**
Having the right people in the room during playbook development workshops is critical. Ideally there should be participation from the business unit’s upper management for overall strategy guidance as well as staff- or supervisor- level individuals for developing detailed recovery procedures.

**The Right Amount of Time**
Depending on the complexity of the business unit, development can take anywhere between 1 and 4 workshops of 1-2 hours each. Knowledge of the business unit helps schedule the right amount of time.

**Risk Assessments**
Risk assessment results help focus the planning efforts on high risk and impact scenarios.

**Business Impact Analyses**
BIAs provide necessary processes information as well as Recovery Time Objectives (RTOs), resource requirements, and interdependencies with other processes or third parties. One of the first steps of playbook development workshops is to review this information with participants and ensure it is still up-to-date.

**The Right Approach**
Beginning workshops with a structured methodology helps guide the conversation and use participants’ time more efficiently.
Practical

Things You Should Be Doing

To help your organization prepare for the changing face of crisis
### Control Environment

Internal audit can help set the organizational tone and influence the crisis management consciousness of its people while providing the required levels of discipline and structure.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📝</td>
<td>Engage the board and executive management in conversations regarding crisis-related risks and potential triggers.</td>
</tr>
<tr>
<td>💬</td>
<td>Leverage the board and audit committee’s expertise and lessons learned on navigating crises.</td>
</tr>
<tr>
<td>📜</td>
<td>Encourage the development a crisis plan and actionable playbook with defined roles and responsibilities for crisis management.</td>
</tr>
<tr>
<td>🚭</td>
<td>Help management define crisis and distinguish between routine and novel crisis and applicable response mechanisms.</td>
</tr>
</tbody>
</table>
Internal Audit can help organizations identify the myriad of external and internal risks that the achievement of strategic and operational objectives.

- Expand the audit universe to include non-traditional and strategic risks such as geo-political, environmental, socio-economic, terrorism, etc.
- Don’t just look at threat risk but also consider missed opportunity risks.
- Conduct surveys to assess crisis risk awareness and readiness throughout the organization.
- Integrate crisis risk assessment into the annual risk assessment efforts.
Control Activities

Assurance regarding the presence and ongoing effectiveness of crisis management procedures at all levels and in all functions of the organization.

- Periodically test the design and operating effectiveness of business continuity, disaster recovery, resilience and crisis management plans.
- Conduct regular simulations testing/validation on established crisis approach.
- Observe and evaluate the completeness and effectiveness of war gaming and simulation testing.
- Consider the prevention, quick response/recovery and resiliency as part of the objectives of internal controls and audit plans.
Information and Communication

Effecting communication to ensure information flows down, across and up the organization as well as with external stakeholders that inform and are impacted by crisis management.

- Provide guidance to management in the development of crisis management framework and capabilities.
- Engage crisis management personnel in internal audit rotations to facilitate knowledge sharing.
- Gather and share crisis management leading practices from outside the organization.
- Develop and communicate using standard and consistent crisis management language.
Ongoing monitoring to assess the quality of the crisis management system's performance over time. Continuous improvement via upstream reporting and implementation of applicable corrective actions.

- Perform post-crisis reviews and assessments.
- Create and roll out a consistent lessons learned approach and methodology for continuous improvement.
- Continuously scan operating environment for potential crisis triggers and understand their impact and ramifications.
- Perform benchmarking of organizational crisis management capabilities and performance.
Recap

Crisis can happen across multiple domains

Risks posed by crisis events are costly, and sometimes detrimental to a business

Internal audit can influence and lead the conversation on Crisis across the organization

An effective crisis framework is built upon a strong foundation of resilience and a realistic crisis management plan

DO: Have a plan and test your plan

DON’T: Get caught off guard
Contact

Ragini Roy Basu, CRM
Principal, Crisis Management
Strategic Risk
Deloitte & Touche LLP
rrbasu@deloitte.com

Linus Akanoh, Jr., CIA, CISA, CGMS, CRMA
Senior Manager, Crisis Management
Strategic Risk
Deloitte & Touche LLP
lakanoh@deloitte.com
Appendix: References for slide #2

Numbers under crisis triggers reflect 2014 statistics

Sources:

Financial disruption: Almost 27,000 business bankruptcies in U.S. alone

Cyber-attacks: Nearly 430 cyber-attacks every week in over 250 companies globally

Confrontations: Nearly 200,000 man-days lost from major work stoppages in the U.S. alone
http://www.bls.gov/news.release/wkstp.nr0.htm

Technological & industrial: 860,000 occupational incidents everyday globally

Misdeeds & financial crime: Almost 90 corporate fraud and embezzlement cases in U.S.
http://www.irs.gov/uac/Statistical-Data-Corporate-Fraud

Other catastrophes: More than 980 events globally
http://www.iii.org/fact-statistic/catastrophes-global
This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2016 Deloitte Development LLC. All rights reserved.

Member of Deloitte Touche Tohmatsu Limited.