eGov@Gujarat

- An e-Governance Bulletin from GUJARAT INFORMATICS LTD.

Vol.7 | No. 7
Jan-Feb, 2010

# Crisis Management Plan (CMP)

CMP



**Courtesy By**

**Shri K. R. Gururaja Rao,**
**Chairman & Managing Director, GIL**

**Dr. Neeta Shah**
**Director (eGovernance)**
**Gujarat Informatics Ltd.**

**Editorial Team**

Mr. Krunal Suthar

## Introduction

Crisis Management is a critical Organizational function. Failure can result in serious harm to stakeholders, losses for an organization, or end its very existence. Public relations practitioners are an integral part of crisis management teams. So a set of best practices and lessons gleaned from our knowledge of crisis management would be a very useful resource for those in public relations. Volumes have been written about crisis management by both practitioners and researchers from many different disciplines making it challenges to synthesize what we know about crisis management and public relations place in that knowledge base. The best place to start this effort is defining critical concepts.

## Definitions of CMP

- A crisis is defined as a significant threat to operations that can have negative consequences if not handled properly. In crisis management, the threat is the potential damage a crisis can inflict on an organization, its stakeholders, and an industry. A crisis can create three related threats: *1) public safety, 2) financial loss, and 3) reputation loss.* Some crisis, such as industrial accidents and product harm, can result in injuries and even loss of lives.

- Crisis can create financial loss by disrupting operations, creating a loss of market share/purchase intentions, or spawning lawsuits related to the crisis. A crisis reflects poorly on an organization and will damage a reputation to some degree. Clearly these three threats are interrelated. Injuries or deaths will results in financial and reputation loss while reputations have a financial impact on organizations.

- Effective crisis management handles the threats sequentially. The primary concern in a crisis has to be public safety. A failure to address public safety intensifies the damage from a crisis. Reputation and financial concerns are considered after public safety has been remedied.

- Ultimately, crisis management is designed to project and organization and its stakeholders from threats and/or reduces the impact felt by threats.

- Crisis management is a process designed to prevent or lessen the damage a crisis can inflict on an organization and its stakeholders. As a process crisis management is not just one thing. Crisis management can be divided into three phases:

  - ✓ *Pre-Crisis*
  - ✓ *Crisis response*
  - ✓ *Post crisis*

- The ***Pre-crisis*** phase is concerned with prevention and preparation. The ***Crisis response*** phase is when management must actually respond to a crisis. The ***Post-crisis*** phase looks for ways to better prepare for the nest crisis and fulfills commitments made during the crisis phase including follow-up information. The tri-part view of crisis management serves as the organizing framework for this entry.

## Purpose of Crisis Management Plan

- To ensure that interruption or manipulations of critical functions/services in critical sector organizations are brief, infrequent and manageable and cause least possible damage.

- To enable respective administrative Ministries/Departments to draw-up their own contingency plans in line with Crisis Management Plan for countering cyber attacks and cyber terrorism, equip themselves suitably for implementation, implement, supervise implementation and ensure compliance among all the organizational units (both public & private) within their domain.

- To assist organizations to put in place mechanisms to effectively deal with cyber security crisis and be able to pin point responsibilities and accountabilities right down to individual level.

## Types of different Crisis

- Crises have many sources, some of which are common to all organizations. Others are specific to certain industries. For directors, it may be helpful to consider them as fitting into one of three groups, based on their severity, frequency and timing:

- **Operational crises** are the day-to-day, minor crises of running the organization and serving individual customers. With good management these can be avoided or promptly resolved.

- **Sudden crises** are events that occur unexpectedly and have a major effect on the organization. These include natural disasters, sabotage and outages of vital services such as power, water or computers. The CEO should have plans for managing crises and business continuity and test the plans through realistic scenario-based simulations.

- **Potential crises** are serious problems that grow larger over time and become critical if they are not addressed. They include declining sales, profits and share prices, failure to respond to new competition, investigations by regulators, and financial difficulties. These problems affect the long-term viability of the entire organization and should be addressed by the CEO through the strategic planning and risk management processes. These groupings of crises are linked. For example:
  - ✓ Operational crises may be symptoms of potential crises.

## Cyber Security Crisis, Possible Targets and Impact

- **Targeted Scanning and Probing of IT infrastructure**
  - ✓ **Possible Targets** - *Sensitive Government and Critical Information infrastructure including*
  - ✓ **Related Impact** - *Pre-cursor to hacking and focused attack leading to cyber crisis*
- **Large scale defacement and semantic attacks on websites**
  - ❖ **Possible Targets**
  - ✓ *High profile national websites such as President, Prime Minister, Parliament, India Portal*
  - ✓ *Websites of Ministries and Financial sector websites*

❖ **Related Impact**

✓ *Huge national embarrassment*

✓ *Total/partial disruption of services, Monetary loss*

- **Malicious Code attacks (i.e. Virus, Worm, Trojans, Botnets)**

❖ **Possible Targets**

✓ *Large & key national/financial databases such as tax information network, citizen database, passports, reservations, banks/FIs, stock exchanges.*

❖ **Related Impact**

✓ *Partial or No response from Computer system*

✓ *Total/partial corruption of data bases*

✓ *Monetary loss, damage to reputation, loss of image etc.*

- **Identity Theft Attacks Large scale spoofing**

❖ **Possible Targets**

✓ *High profile users in Govt., Corporate and key economic installations*

✓ *Websites of financial and critical sectors*

❖ **Related Impact**

✓ *Increased possibility of identity theft leading to penetration into sensitive IT systems and Databases*

✓ *Loss of sensitive data, monetary loss and loss of image.*

- **Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks**

❖ **Possible Targets**

✓ *Public utility services*

✓ *Critical systems*

✓ *Supervisory Control and Data Acquisition (SCADA) System*

✓ *Banks/FIs, Insurance, stock exchange, online reservations*

❖ **Related Impact**

- ✓ *Total/partial disruption of services for prolonged periods*
- ✓ *Possible damage to life and/or property*
- ✓ *Monetary loss, damage to reputation, loss of image etc*

- **Infrastructure attacks**

❖ **Possible Targets**

- ✓ *Control systems of power, petroleum, transport, air traffic control, refineries, fertilizers etc and all process industries*
- ✓ *International gateways/ISPs*
- ✓ *DNS servers*

❖ **Related Impact**

- ✓ *Total/partial disruption of services/activities in one or more critical*
- ✓ *Huge economic fallouts*
- ✓ *Illegal diversion of Internet and mail traffic to some other countries*

- Cyber security crisis may be triggered by attacks on
  - ✓ *Individual IT systems*
  - ✓ *simultaneously on multiple IT systems*
  - ✓ *IT networks in a single or multiple organizations, states or entire nation from within or outside the country*
- Consequences of disruptions may threaten lives, economy and national security.
- It may origin from places within the country or anywhere outside the country Attack source may spread geographically across the globe

## Crisis Recognition, Mitigation and Management

- **Level of concern**

**Level 1 Guarded**

**Scope: Individual Organization**

- ✓ Large scale attacks on the IT infrastructure of an organization

**Level 2 Elevated**

**Scope: Multiple Organizations**

- ✓ Simultaneous large scale attacks onto IT infrastructure of multiple organizations

**Level 3 Heightened**

**Scope: State/Multiple States**

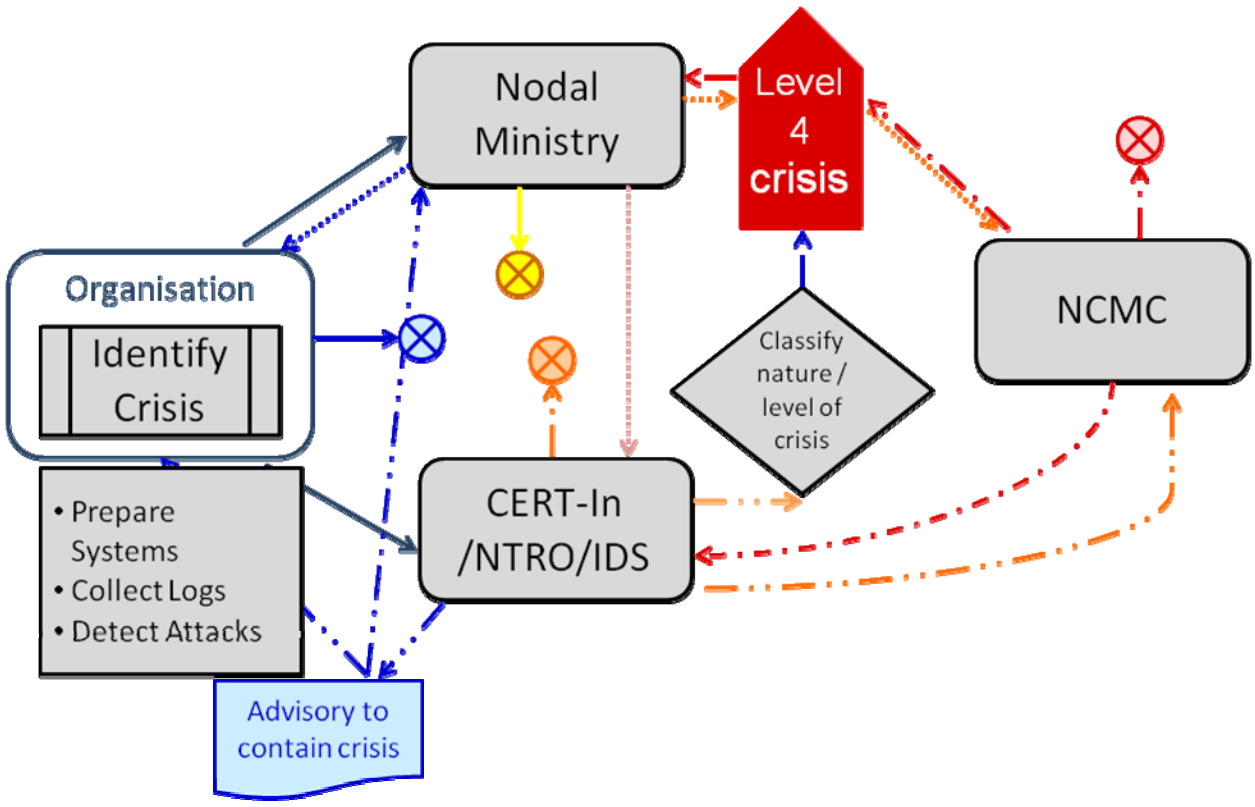
- ✓ Cyber attacks on infrastructure of critical sector and Government across a state or multiple states.

**Level 4 Serious**

**Scope: Entire Nation**

- ✓ Cyber attacks on infrastructure of critical sector and Government across the nation.

**Crisis Management - Response Flow**



**Incident Response and Mitigation**

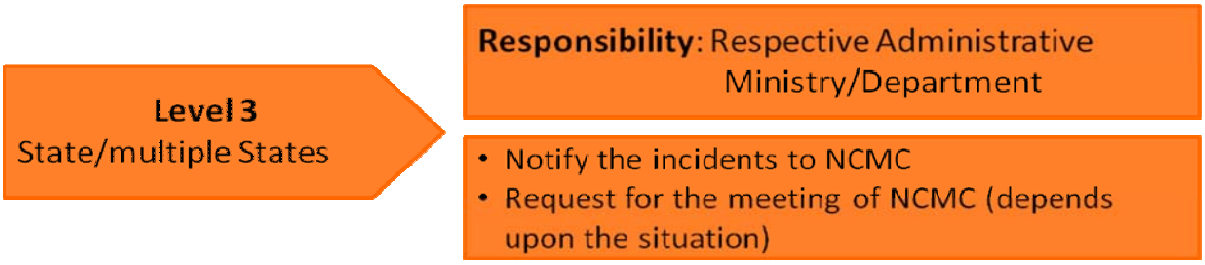
**Level-1**


- ✓ *Notify incidents to respective administrative Ministry/Department*
- ✓ *Monitor and detect anomalous behavior and degradation of services*
- ✓ *Take all logs of affected systems for forensics analysis*
- ✓ *Notify and send relevant information to CERT-In/ NTRO/MoD, IDS (DIARA)*
- ✓ *Implement appropriate eradication process and recovery of systems as prescribed against each type of attack*

**Level-2**

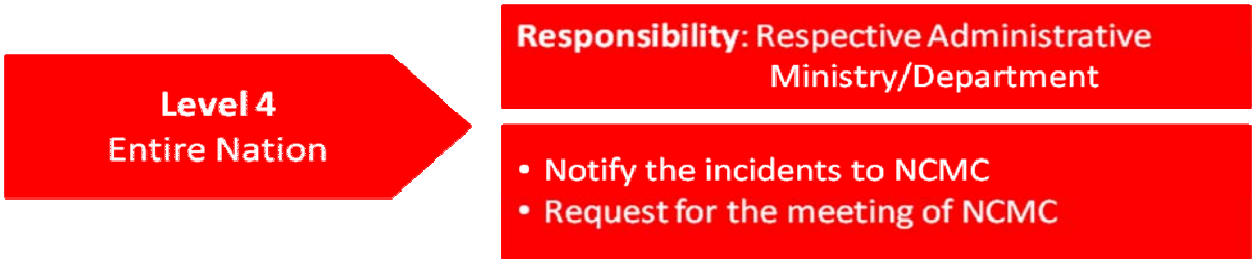

- ✓ *Notify incidents to respective administrative Ministry/Department*
- ✓ *Monitor and detect anomalous behavior and degradation of services*
- ✓ *Take all logs of affected systems for forensics analysis*
- ✓ *Notify and send relevant information to CERT-In/ NTRO/MoD, IDS (DIARA)*
- ✓ *Implement appropriate eradication process and recovery of systems as prescribed against each type of attack*

**Level-3**




- ✓ Implement the Contingency Plan
- ✓ Deploy onsite response team on 24X7 basis
- ✓ Limit the access to systems and networks from outside in consultation with ISPs.
- ✓ Implement the appropriate eradication process and recovery of systems

**Level-4**




- ✓ Carry out all the steps as indicated in level 3
- ✓ Implement directives of NCMC, respective administrative Ministry/Department
- ✓ Implement specific advisories and instructions issued by CERT-In, NTRO, MoD and other designated agencies.

## Structure of Crisis Management Plan

- The structure of Crisis Management Plan for countering Cyber Terrorism has five sections dealing with the following:

  - ✓ *Concept of Crisis Management Plan*
  - ✓ *Nature of cyber crisis*
  - ✓ *Incident prevention measures*
  - ✓ *Crisis recognition mitigation and management*
  - ✓ *Incident closure and information sharing*

In addition, the document contains guidelines on:

- ✓ *Implementing Information Security Management System (ISMS)*
- ✓ *Incident Response Activities in first hour and first 24 hours*
- ✓ *Crisis Management and Security of Critical Infrastructure*

## Implementation of Crisis Management Plan

- Draw up your own sectoral Crisis Management Plan inline with the Crisis Management Plan approved by NCMC
- Implement Information Security Management System as per ISO 27001 standard to prevent cyber security incidents

- Convey
  - ✓ *Specific feedback on Crisis Management Plan*
  - ✓ *Any difficulties/issues in implementation of Crisis Management Plan*
- Seek help and advice as necessary to develop and implement sectoral Crisis Management Plan
- Use the remote security profiling service of CERT-In to improve security posture
- Participate in the CMP mock drills to be conducted by CERT-In
- Participate in the early watch and warning efforts of CERT-In to receive timely advice
- Organize sectoral workshops to communicate and guide all relevant organizations in your constituency to draw up their own Crisis Management Plan and implement the same

Crisis management & Emergency response is a set of actions aimed at rapid response & remedial measures and recovery & restoration of normalcy in the event of a build-up or emergence of a crisis.

These actions include:

- ✓ *Containment of crisis*
- ✓ *Communication to all concerned and*
- ✓ *Coordination of efforts*

that can facilitate,

- ✓ *Adequate & swift response in a timely manner*
- ✓ *Business continuity to maintain availability of minimum essential services/activities*
- ✓ *Detailed analysis of the crisis event, initiation of appropriate disaster recovery measures and return to normalcy at the earliest*
- ✓ *Learning from the crisis*

*Crisis management and emergency response* involves actions at **two levels**:

- *Actions within an organization*
  - ✓ *the point of action where the crisis has occurred (as part of due diligence and fulfillment of its business objectives, legal and commercial obligations)*
- *Actions beyond an organization*

- ✓ *the point of coordination between multiple agencies & take holders (in view of public safety, economic order and national security)*

## Points for action of CMP

**Organization level CMP – Points for action**

- Identify a member of senior management as a 'Chief Information Security Officer (CISO)' to coordinate security policy compliance efforts across the organization and interact regularly with CERT-In and sectoral 'Point of Contact'.
- Establish a Crisis Management Group, on the lines of Sectoral Crisis Management Committee, with head of organization as its Chairman.
- Prepare a list of contact persons complete with up-to-date contact details.
- Prepare an Organizational level CMP on the lines of CMP of CERT-In, outlining roles, responsibilities of organizational stakeholders, CMP coordination process.
- Implement the CMP, including security best practices and specific action points as outlined below:
  - ✓ *Prepare a Security plan and implement Security control measures as per ISO 27001 and other guidelines/ standards as appropriate*
  - ✓ *Carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with business impact assessment and criticality of business functions*
- Develop and implement a business continuity strategy and contingency plan for IT systems.
- Develop and implement ICT disaster recovery and security incident management processes.
- Periodically test and evaluate the adequacy and effectiveness of technical security control measures, especially after each significant change to the IT applications/systems/networks and it can include:
  - ✓ *Penetration testing (both announced and unannounced)*
  - ✓ *Vulnerability assessment*
  - ✓ *Application security testing*
  - ✓ *Web security testing*
- Carry out audit of information infrastructure on an annual basis and when there is a major upgradadtion/change in IT infrastructure, by an independent IT security auditing organization (Ref. to list of CERT-In empanelled IT security auditors on CERT-In web site at http://www.cert-in.org.in).
- Report to CERT-In cyber security incidents as and when they occur and status of cyber security periodically and take part in cyber security mock drills.

## Sectoral level CMP – Points for action

- Identify a member of senior management as a '*Point of Contact*' to coordinate security policy compliance efforts across the sector and interact regularly with CERT-In.
- Establish a Sectoral Crisis Management Committee, on the lines of National Crisis Management Committee, with Secretary (in case of Central Ministries/Depts) or Chief Secretary (in case of Sates/UTs) as its Chairman and a 24x7 control room to monitor crisis situations.
- Prepare a list of organizational units that fall under the purview of sectoral CMP and provide them with a list of action points for compliance.
- Direct the organizational units to identify and designate a member of senior management as '**Chief Information Security Officer (CISO).**
- Prepare a list of CISOs complete with up-to-date contact details.
- Prepare a sectoral CMP on the lines of CMP of CERT-In, outlining roles, responsibilities of sectoral stakeholders, CMP coordination process.
- Direct the organizational units to develop and implement their own CMP on the lines of CMP of CERT-In, including security best practices as per ISO 27001 and report compliance on a periodic basis.

# eGovernance News

## 13th National e-Governance Conference 2009-10

The Department of Administrative Reforms & Public Grievance, Government of India, has been organizing the National Conference on eGovernance every Year.

The 13th National Conference on e-Governance organized by Department of Administrative Reforms & Public Grievance, Department of Information Technology, Government of India in collaboration with State Government of Rajasthan on 18th & 19th February, 2010 at Birla Auditorium, Jaipur, Rajasthan.

The theme for this year's conference was "**e-Governance from Citizen's Perspective"** which will explore how use of ICT has transformed governance from the perspective of the beneficiaries of the services. The focus sector for this year's conference is Education with the agenda "ICT in Education-enhancing quality and reach".

Gujarat State had won following two (2) awards

| Sr. No | Name of Project nominated for Award | Category |
|---|---|---|
| 1. | XGN (xTENDED gREEN nODE) | Excellence in Government Process Re-engineering |
| 2. | ICT in Gujarat Judiciary | Outstanding Performance in Citizen-Centric Service Delivery |
| | | Exemplary Horizontal Transfer for ICT-based Best Practice |

# Web Corner

Crisis Management Plan

http://www.cert-in.org.in

***For electronic subscription to the bulletin, please email us with your email address at:***

***info@gujaratinformatics.com***

***Or visit us at:***

***www.gujaratinformatics.com***

**Contact Address:**

**Gujarat Informatics Ltd.**
**Block No. 1, 8th Floor,**
**Udyog Bhavan,**
**Gandhinagar – 382010**
**Phone: 079 – 23256022**
**Fax: 079 – 23238925**