Cyber Crisis Management Plan
for
Countering Cyber Attacks and Cyber Terrorism

Savita Utreja, Scientist 'F' (sutreja@meity.gov.in)
Indian Computer Emergency Response Team(CERT-In)
Ministry of Electronics & Information Technology (MeitY)

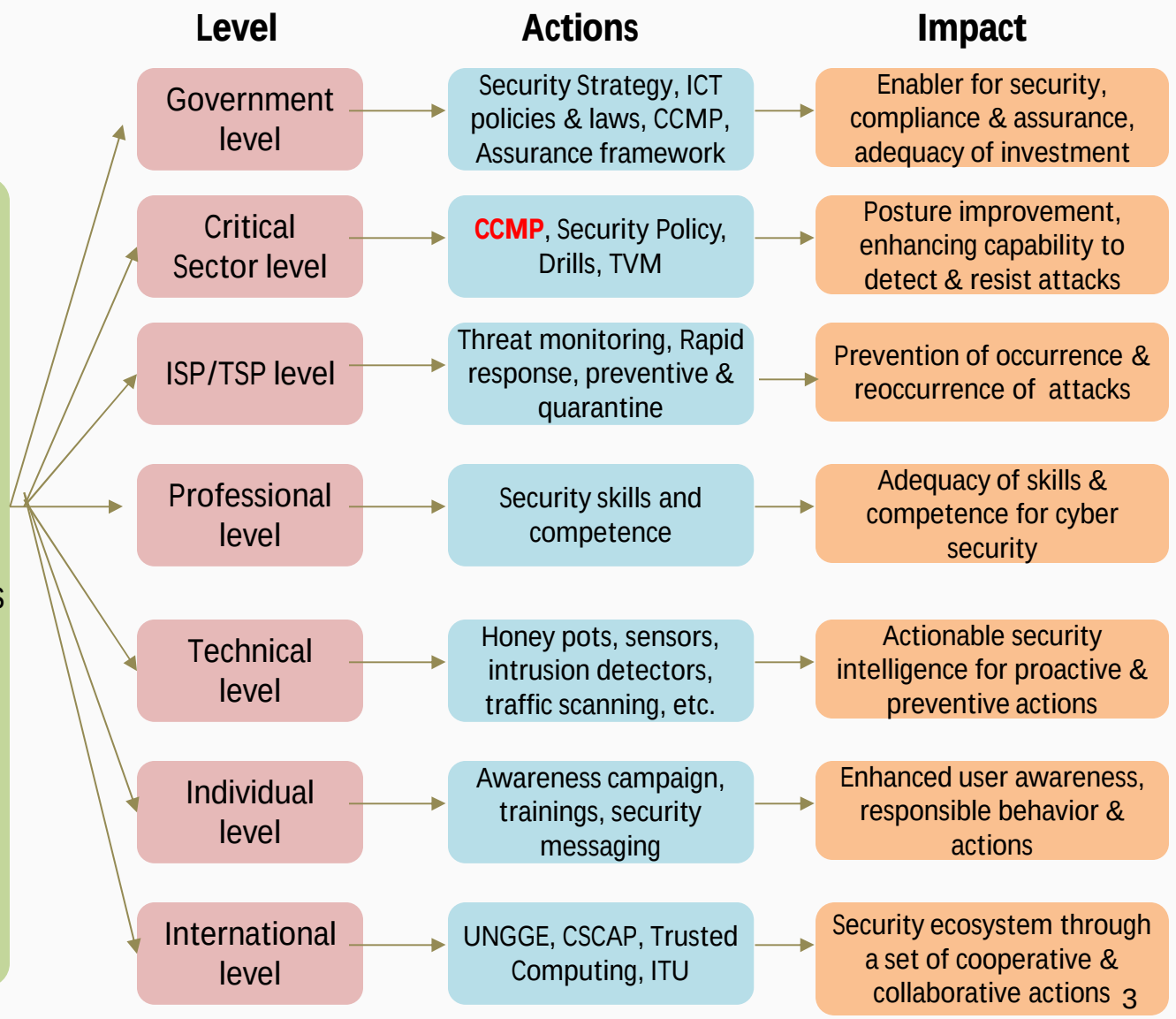
Outline

- Cyber Crisis Management Plan – Purpose
- Cyber Crisis Management Plan – Mandate
- Structure of Cyber Crisis Management Plan
- Cyber Crisis Management Plan – Points of Actions
- Cyber Security Drills

Actions for Cyber Security

Perspectives for effective security of cyber space

- Strategic
- Legal
- Protection
- **Crisis response and resolution**
- Compliance
- Education & Awareness
- Enforcement perspective
- Collaboration
- Data Security and Privacy



Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism

Cyber Crisis Management Plan - Purpose

- The purpose of this plan is to establish the strategic framework and guide actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident.
- To ensure that interruption or manipulations of critical functions/services in critical sector organisations are brief, infrequent and manageable and cause least possible damage.
- 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.

Cyber Crisis Management Plan - Mandate

- Ministries/Departments of Central Govt., State Govts. and Union Territories to draw-up their own sectoral Cyber Crisis Management Plans in line with the Cyber Crisis Management Plan for Countering Cyber attacks and Cyber Terrorism

- Equip themselves suitably for implementation, supervise implementation and ensure compliance among all the organizational units (both public & private) within their domain

- CERT-In/ MeitY to conduct mock drills with Ministries/organisations

- MeitY to seek necessary compliance information on implementation of the best IT security practices from all the organizational units of the Ministries/Departments of Central Government, State Governments and Union Territories on a regular basis and apprise the NCMC of progress

Concept of Cyber Crisis Management Plan

- The Cyber Crisis Management Plan provides the strategic framework and guides actions to prepare for, respond to, and begin to coordinate recovery from a cyber incident.

- Covers different type of cyber crisis, possible targets and related impact, actions and responsibilities of concerned stakeholders, cyber incident response coordination among Ministries/Departments of Central Government, its agencies and Critical Information Infrastructure organizations to deal with cyber crisis situations.

- The field of cyber security is technology intensive and new vulnerabilities emerge with progress in technology giving rise to new types of incidents. As such, the plan of response to cyber security incidents need to be updated on regular basis, preferably once in a year.

Nature of Cyber Crisis and Contingencies

- Cyber attacks may be triggered on
  - Individual systems
  - Multiple systems and networks in a single or multiple organizations
  - States and entire Nation

- Targeted cyber attacks on infrastructure of one or more critical sectors, either individually or simultaneously, may result in significant/complete breakdown of supplies or services essential to the life of the citizens including but not limited to Finance, Defence, Transport, Energy, Communication or critical sector. These events would lead to National Crisis.

Nature of Cyber Crisis and Contingencies

- Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure
- Large scale defacement of websites
- Malicious Code attacks (virus/worm/ /Trojans/Botnets)
- Malware affecting Mobile devices
- Large scale SPAM attacks
- Identity Theft Attacks
- Denial of Service(DoS) attacks and Distributed Denial of Service(DDoS) attacks
- Domain Name Server (DNS) attacks
- Application Level Attacks
- Cyber Espionage and Advanced Persistent Threats

Cyber Security Threat Landscape

Top Threats 2016	Assessed Trends 2016
1. Malware	
2. Web based attacks	
3. Web application attacks	
4. Denial of service	
5. Botnets	
6. Phishing	
7. Spam	
8. Ransomware	
9. Insider threat (malicious, accidental)	
10. Physical manipulation/damage/ theft/loss	
11. Exploit kits	
12. Data breaches	

Cyber Security threat landscape

- Attack Targets
  - Critical infrastructure
  - Business intelligence
  - Personally identifiable information
- Attack Motives
  - Disruption of Services
  - Cyber espionage
  - Financial frauds
- Attack Actors/elements
  - Nation states
  - Cyber criminals
  - Hacker groups
  - Malicious Insiders
- Attack vectors and medium
  - Botnets
  - Vulnerabilities and Exploit tool kits
  - Social engineering
  - Ignorant users

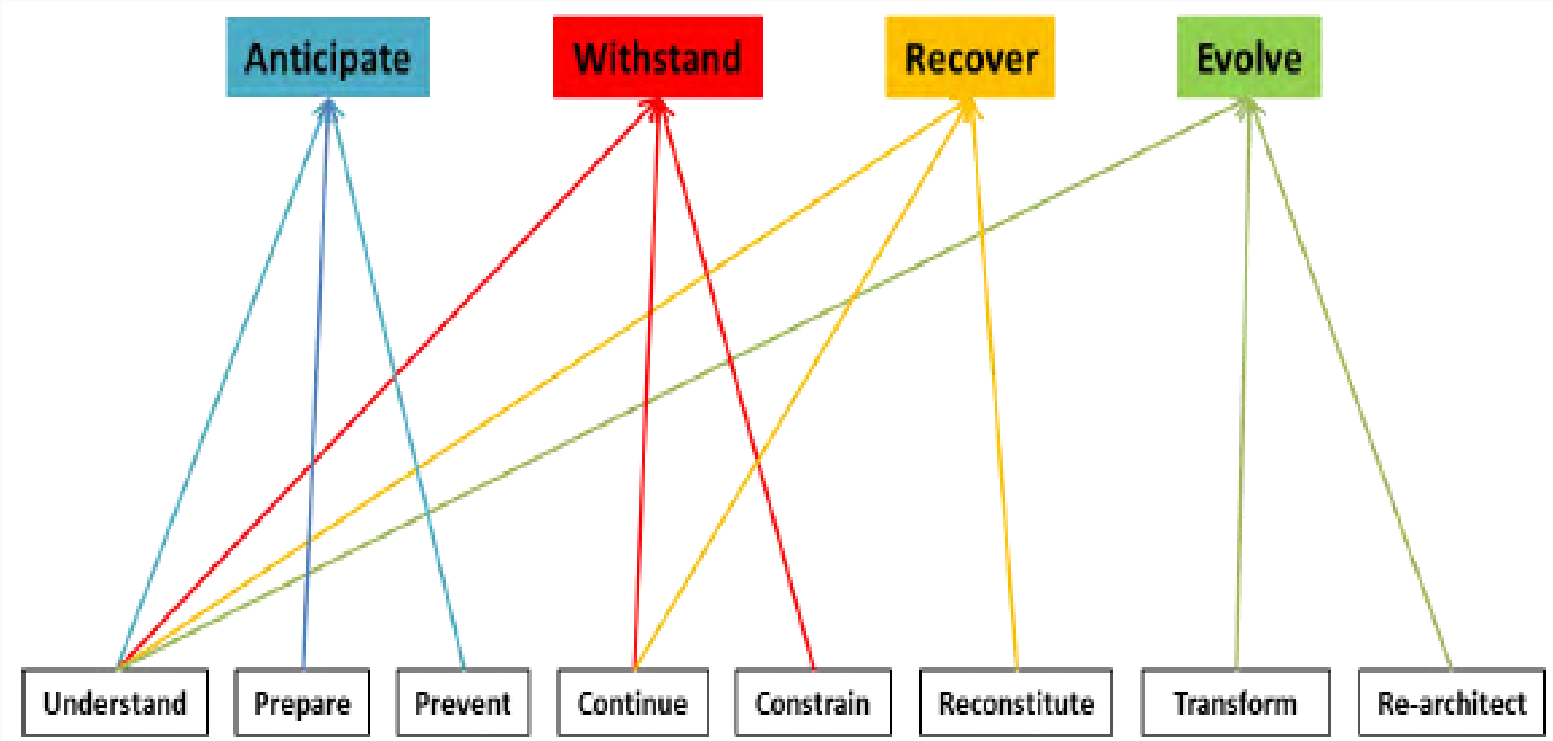
Building Cyber Resilience

Cyber Resilience

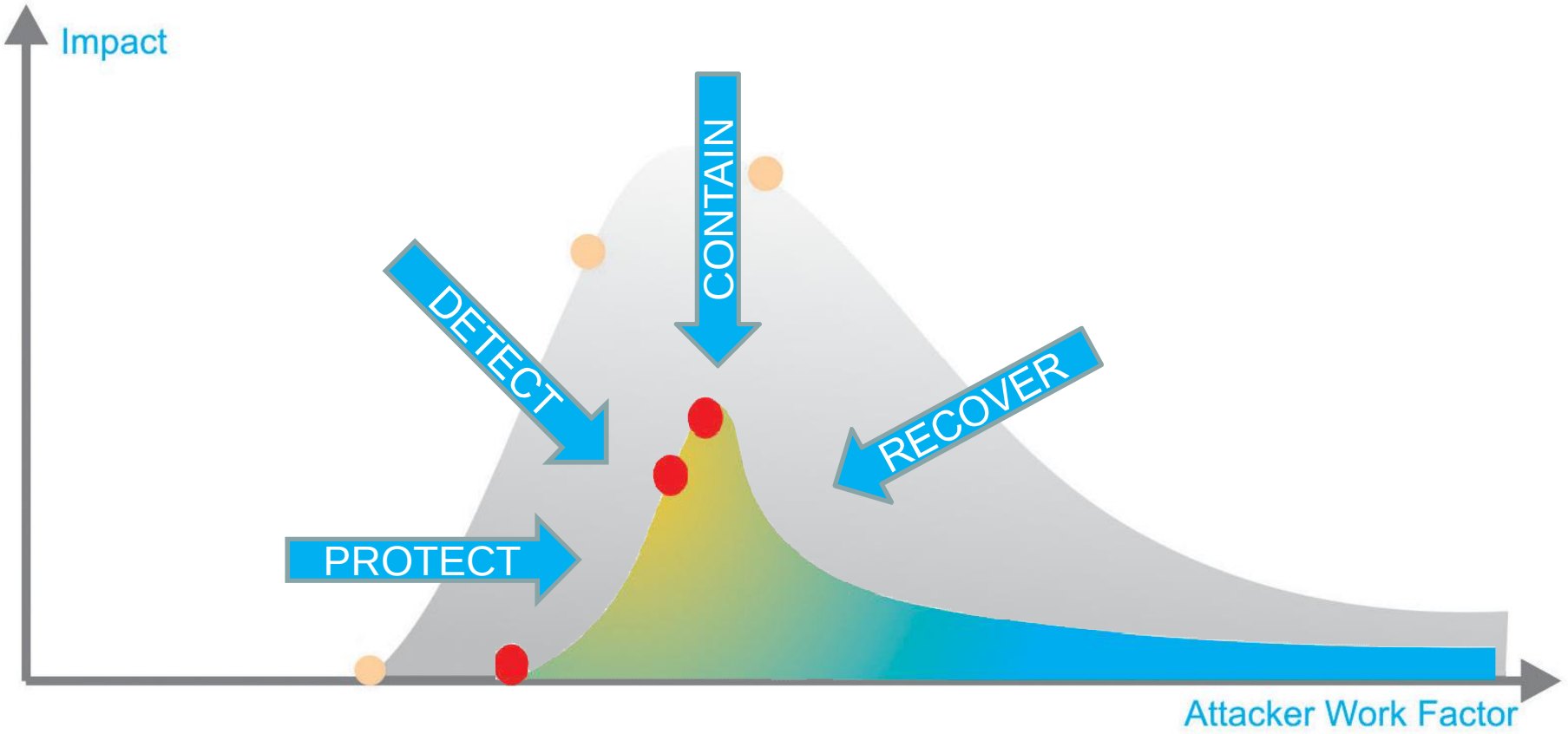
Cyber resilience is defined as ability of organization or business process to

- Anticipate: Maintain a state of informed preparedness in order to forestall compromises of mission/business functions from adversary attacks
- Withstand: Continue essential mission/business functions despite successful execution of an attack by an adversary
- Contain: Localize containment of crisis and isolate trusted systems from untrusted systems to continue essential business operations in the event of cyber attacks
- Recover: Restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary
- Evolve: To change missions/business functions and/or the supporting cyber capabilities, so as to minimize adverse impacts from actual or predicted adversary attacks

Cyber resiliency goals and principles



Effective Resilience v/s Impact of Cyber Attack



Incident Prevention

Prevention and Precautionary Measures

- Nomination of Chief Information Security Officer
- Information Security Policy & implementation of best practices
- Business Continuity Plan(BCP)
- Disaster Recovery Plan (DRP)
- Security of Information infrastructure and network
- Network traffic scanning
- Isolation of critical networks
- Implementation of Security guidelines issued by concerned authorities
- Background checks
- Audit & Assurance
- Security training & awareness
- Sharing of information pertaining to incidents

Self- Assessment Questionnaire

S. No.	QUESTION	Yes/No/In Process/Not aware of	Comment
1	Whether Chief Information Security Officer (CISO) has been nominated for the organization?		
2	Whether organisation is aware of IT Security best practices & has documented its Information Security policy/ procedures?		
3.	Whether compliance to IT security best practices has been verified by the organization by self-assessment or by third party on periodic basis?		
4.	Whether IT security audit is conducted by the organization by third party on periodic basis? (by way of security testing of IT infrastructure involving Code Review/Vulnerability assessment and/or Penetration Testing)		
5.	Whether CMP document has been developed and implemented within the organisation?		
6.	Whether the organization is aware of cyber security drills conducted by CERT-In and has ever participated or plans to participate in the drill?		
7.	Are the advanced security devices like IDS/IPS and SIEM(Security information & event manager) etc deployed in the organization? If yes, whether their reports are analysed on regular basis ?		
8.	Whether the organization has mechanism for collaboration and sharing of security analysis reports (Malicious activity logs, Advanced level malware, Analysis reports of IDS/IPS, firewall etc) with CERT-In/Sectoral CERTs etc.?		
9.	Whether the organization has mechanisms for analysing the data collected from different security devices to identify the upcoming threats in future and take appropriate actions to mitigate the upcoming threats and identified vulnerabilities?		

Self- Assessment Questionnaire

On the basis of responses above, Please tick (√) from the following options to indicate the level of compliance achieved or ' in process' for your organizations:
Level 1 achieved or in process- (if answers for s.no. 1 and 2 is yes or "in process")

Level 2 achieved or in process-(if answers for s.no. 1 to 3 is yes or "in process")

Level 3 achieved or in process-(if answers for s.no. 1 to 4 is yes or "in process")

Level 3+ achieved or in process-(if answers for s.no. 1 to 6 is yes or "in process")

Level 4 achieved or in process-(if answers for S.no. 1 to 7 is yes or "in process")

Level 4+ achieved or in process-(if answers for S.no. 1 to 8 is yes or "in process")

Level 4++ achieved or in process- (if answers for S.no. 1 to 9 is yes or "in process")

Any additional points related to implementation of Information Security best practices at your organization:

<Name of Central Govt. Ministry/Department/State Government/ Organization> has achieved / in process of achieving …….. level of compliance with respect to implementation of security best practices.

Crisis Recognition, Mitigation and Management

Levels of concern

Threat Level	Condition
Level 1 Guarded Scope: Individual Organisation	Large scale attacks on the IT infrastructure of an organisation
Level 2 Elevated Scope: Multiple Organisations	Simultaneous large scale attacks onto IT infrastructure of multiple organisations
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.

Incident Response and Mitigation

Level 1
Individual Organisation

Responsibility: Affected Organisation

- 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

Incident Response and Mitigation

Level 2
Multiple Organisations

Responsibility: Respective Administrative Ministry/Department

- 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

Incident Response and Mitigation

Level 3
State/multiple States

Responsibility: Respective Administrative Ministry/Department

- Notify the incidents to NCMC
- Request for the meeting of NCMC (depends upon the situation)

- 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

Incident Response and Mitigation

Level 4
Entire Nation

Responsibility: Respective Administrative Ministry/Department

- Notify the incidents to NCMC
- Request for the meeting of NCMC

- 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.

Cyber Crisis Management & Emergency Response

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 in accordance with international best practices and industry accepted standards
- Detailed analysis of the crisis event, initiation of appropriate disaster recovery measures and return to normalcy at the earliest
- Learning from the crisis

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

- Actions within an organisation – the point of action where the crisis has occurred
- Actions beyond an organisation – the point of coordination between multiple agencies & stakeholders *(in view of public safety, economic order and national security)*

Actions within an organisation are of three types:

- Putting in place systems and procedures in the form of a crisis management plan in accordance with accepted international best practices
- Ensuring complete alignment with the National Crisis Management Plan prepared by CERT-In/MeitY for countering cyber attacks and cyber terrorism
- Implementing the crisis management plan, verifying workability through tests & mock drills and demonstrating compliance

How can we work together for effective Cyber Crisis Management

Effective Cyber Crisis management & emergency response in an organisation depends on:

- Proactive security incident preventive actions in the form of implementation of Information Security management System (ISMS) as per ISO 27001:2013 standard
- Proactive monitoring of network assets and traffic for any visible signs of changes from normal situation
- Being in continuous touch with CERT-In/NTRO/IDS(DIARA) to receive actionable cyber security alerts and advice

Cyber Crisis Management & Emergency Response

Organisations can make effective use of CERT-In supportive initiatives such as:

- Empanelment of IT security auditors to verify effective implementation of technical, managerial and operational security controls
- Proactive and timely security alerts and advices to remain fully updated with regard to possible virus/worm infections, latest security patch status and workarounds for zero-day exploits

Specific assistance in Cyber Security Crisis Management and Emergency Response

- Development and implementation of sectoral cyber crisis management plan (CCMP) in line with National cyber crisis management plan (CCMP) of CERT-In.
- Remote profiling of IT systems and Networks to determine the security posture.
- Cyber Security drills to enable participating organisations to assess their preparedness in the event of cyber attacks.

Organisations can help CERT-In in securing the cyber space by:

- Duly reporting security incidents and sharing all relevant information that can support real-time incident analysis & rapid response

- Collaborating with CERT-In to keep a watch on cyber space to look for malicious traffic, virus/worm infections and visible signs of build-up or emergence DDoS attacks

- Regularly participating in CERT-In trainings/workshops on contemporary topics/issues to remain updated on technology and security best practices

Points of action for Sectoral/ Organizational CCMP

Sectoral 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 Cyber 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 organisational units that fall under the purview of sectoral CMP and provide them with a list of action points for compliance
- Direct the organisational 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 CCMP on the lines of CCMP of CERT-In, outlining roles, responsibilities of sectoral stakeholders, CMP coordination process
- Direct the organisational units to develop and implement their own CCMP on the lines of CCMP of CERT-In, including security best practices as per ISO 27001 and report compliance on a periodic basis
- Participate in the cyber security drills to be conducted by CERT-In on a regular basis

Organisation level CCMP – Points for action

- Identify a member of senior management as a 'Chief Information Security Officer (CISO)' to coordinate security policy compliance efforts across the organisation and interact regularly with CERT-In and sectoral 'Point of Contact'

- Establish a Cyber Crisis Management Group, on the lines of Sectoral Crisis Management Committee, with head of organisation as its Chairman

- Prepare a list of contact persons complete with up-to-date contact details

- Prepare an Organisational level CCMP on the lines of CCMP of CERT-In, outlining roles, responsibilities of organisational stakeholders, CCMP coordination process

- Implement the CCMP, 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

Organization level CCMP – Points for action

- 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 upgradation/change in IT infrastructure, by an independent IT security auditing organisation *(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

Cyber Security Drill - Concept

Based on the nature and objective of drills, following levels of drills are designed by CERT-In:

- Layer-I exercise is basic level of drill which is focused on improving information security awareness and concept of drill.

- Layer II exercise involved launching simulated attacks on homogenous / heterogeneous environment of drill setup at organization premises which is separate from production network. Enabling the participating organizations to assess their attack defence, detection, recovery and incident response capabilities.

- Layer III exercise involved launching of the injects to participating organizations based on hypothetical and/or hybrid scenarios (Hypothetical + Simulated attack). Enabling the participating organizations to assess the effectiveness of their incident response and recovery procedures and reinforce their coordination with internal as well as external stakeholders including CERT-In.

Reference Standards & Guidelines

In addition to CCMP of CERT-In, the following docs can be referred:

- Information security management systems Requirements – ISO 27001:2013
- Code of practice for information security management – ISO 27002:2013
- Information security management system implementation guidance – ISO 27003:2010
- Security risk assessment – ISO 27005:2011
- Business continuity management strategy – ISO 22301:2012
- Contingency planning guide for IT systems – NIST SP 800-34
- ICT Disaster recovery services – ISO 24762:2008
- Information Security incident management – ISO/IEC 27035:2011
- CIS 20 most important security controls and metrics for effective cyber security and continuous security policy compliance (Prioritizing security baselines)

Thank you