CERT-MU

Computer Emergency Response Team of Mauritius

National Cyber Crisis Management Plan

Instructors:

Dr. Kaleem Ahmed Usmani

Mrs. Jennita Appayya

TLP: White

Part 3

Implementation, Testing and Maintaining the plan

Implementation, Testing and Maintaining a National Cyber Crisis Management Plan

- Today's training session aims to elaborate on how to implement, test and maintain a National Cyber Crisis Management Plan after its development.
- The focus will be on the importance of testing a National Cyber Crisis Management Plan and why should the plan must be reviewed.

CERT-MU

Implementation, Testing and Maintaining a National Cyber Crisis Management Plan

Implementation of the National Cyber Crisis Management Plan

After the National Cyber Crisis Management Plan has been developed and approved by the Government , its implementation and execution starts. It consists of the following steps:

- Setting up of the governance committee which will be responsible for overseeing the execution of the NCMP and facilitating monitoring, control and transmission of decisions
- Formation of the Incident Coordination and Communication Team
- Venue for holding meetings during a cyber crisis
- Testing of the NCMP
- Regular review of the plan

Testing the National Cyber Crisis Management Plan

- After the implementation process, the next step is to test the plan.
- Until the plan is not tested, it will not be effective.
- Testing the plan yield two important results:
    - ➢A clear understanding of whether your plan is likely to work and
    - ➢Identification of the gaps in the plan and address them accordingly

CERT-MU

Testing the National Cyber Cyber Crisis Management Plan

Rationale for testing a National Cyber Cyber Crisis Management Plan:

- To assess the ability of a nation to coordinate response to cyber emergency situations
- To assess the ability of the governing body/committee responsible for national incident response as a leading authority
- To assess the impact of a serious cyber or critical situation affecting a country
- To test tasking and guidance needed to resolve cyber incidents
- To assess strategic information sharing and communication with internal and external stakeholders, partners and other parties
- To identify any gaps in the plan and improve incident resolution

How to Test the National Cyber Crisis Management Plan?

Once there is a clear and documented plan, it could be tested to assess its effectiveness through **Cybersecurity Exercises** which comprises of:

- Table Top Exercises (TTX) – For the Top Management
  - ➢A security incident preparedness activity, taking incident coordination team through the process of dealing with a simulated incident scenario.
- Technical exercises – For the Incident Response Team
  - ➢Another effective way to test the incident response plan is to simulate a real attack to see how stakeholders of the plan will respond. These tests not only evaluate what incident coordination team would do when faced up against a major incident, but how they would do it.

Execution of the National Cyber Crisis Management Plan

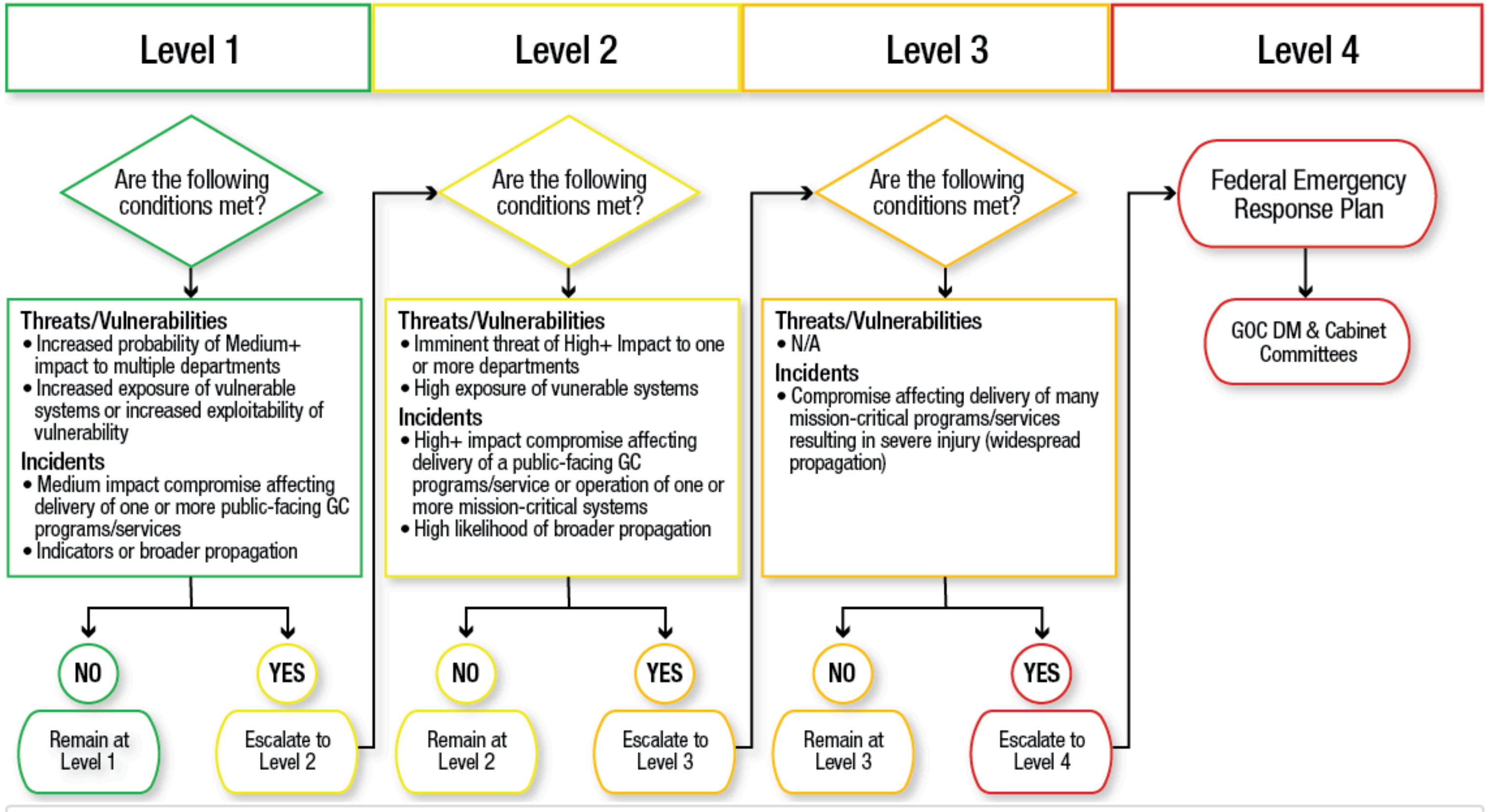
- Execution of a National Cyber Crisis Management Plan consists of the steps the nation will take when an incident of national significance has been detected.
- This phase activates the NCIRP and involves invoking all the measures listed in the plan.

Execution of the National Cyber Incident Response Plan

Example: Canada

Execution of the National Cyber Incident Response Plan during a cyber crisis

Figure 5: Escalation and response levels



Level 1

Are the following conditions met?

Threats/Vulnerabilities
- Increased probability of Medium+ impact to multiple departments
- Increased exposure of vulnerable systems or increased exploitability of vulnerability

Incidents
- Medium impact compromise affecting delivery of one or more public-facing GC programs/services
- Indicators or broader propagation

NO – Remain at Level 1

YES – Escalate to Level 2

Level 2

Are the following conditions met?

Threats/Vulnerabilities
- Imminent threat of High+ Impact to one or more departments
- High exposure of vunerable systems

Incidents
- High+ impact compromise affecting delivery of a public-facing GC programs/service or operation of one or more mission-critical systems
- High likelihood of broader propagation

NO – Remain at Level 2

YES – Escalate to Level 3

Level 3

Are the following conditions met?

Threats/Vulnerabilities
- N/A

Incidents
- Compromise affecting delivery of many mission-critical programs/services resulting in severe injury (widespread propagation)

NO – Remain at Level 3

YES – Escalate to Level 4

Level 4

Federal Emergency Response Plan

GOC DM & Cabinet Committees

Review and Maintenance of a National Cyber Crisis Management Plan

- For effective incident response at national level, a National Cyber Crisis Management Plan should be reviewed and updated regularly.
- The revision process includes developing or updating any process pertaining to the incident response capabilities which can affect the plan
- Any significant update should be vetted by stakeholders or the governing body or committee responsible for the NCMP

CERT-MU

Review and Maintenance of the National Cyber Crisis Management Plan

A NCMP may be updated and maintained to accomplish the following:

- Assess and update information on the capabilities in support of cyber incident response goals and objectives. A simulation exercise will help for the capability assessment.
- Update processes based on changes in the national cyber threat or hazard environment.
- Incorporate lessons learned and effective practices from day-to-day operations, exercises, and actual incidents and alerts.
- Adapt to opportunities and challenges that arise as technology evolves and changes.
- Reflect progress in the Nation's cyber incident response mission activities, the need to execute new laws and strategic changes to national priorities or national capabilities.

CERT-MU

National Cyber Cyber Crisis Management Plan – The Mauritian Experience

Name: National Cyber Incident Response Plan

- Governance Committee: National Disaster Cybersecurity and Cybercrime Committee (NDCCC – is an apex committee and its role is to coordinate and monitor the cyber crisis situation).

- NDCCC comprise of members from public and private sector . There are 9 permanent and 21 extended members.

- NDCCC is chaired by the Minister of IT or Permanent Secretary depending on the severity of incident.

National Cyber Incident Response Plan – The Mauritian Experience (Contd.)

- The plan defines the Incident Response and Public Relations team. Incident Response Team comprise of national CERT, IT Security Unit of Ministry of IT, Mauritius Police Force and Internet Service Providers.
- Public Relations Team consist of Communication person from the Minister's Office, Government Information System Unit representative of the PMO and also a representative from the incident response team.
- Location to hold meetings during the cyber crisis is the office of the Ministry of IT.

National Cyber Incident Response Plan – The Mauritian Experience (Contd.)

- TLP is used to for the information exchange.
- Five level of severity is defined.
- Level 2 severity incidents will be coordinated under the chairmanship of the PS.
- Level 3-5 severity incidents will be coordinated under the chairmanship of the Minister.
- Testing of the plan has been done.
- Helpdesk provision has been made at the level of CERT-MU
- Execution is planned.

CERT-MU

National Cyber Incident Response Plan – Important Considerations (Contd.)

- To setup a national level committee with members who have the experience and understanding of cyber threat handling and resolution.

- To assess the capacity of the team which will deal with incident during the cyber crisis.

- To assess the information sharing and communication efficiency of the public relations team.

CERT-MU

Thank You

CONTACT US

Computer Emergency Response Team of Mauritius (CERT-MU)

Tel: 210 55 20 | Hotline: 800 2378

General Enquiry: contact@cert.ncb.mu
Subscribe to Mail List: subscribe@cert.ncb.mu

Incident Reporting: incident@cert.ncb.mu
Vulnerability Reporting: vulnerability@cert.ncb.mu

Cybersecurity Portal: http://cybersecurity.ncb.mu
Website: www.cert-mu.org.mu