Request For Information On: NIST Incident Co-ordination and Handling

Name: Vishwas Rudramurthy

Name of the Organisation: C.I.G.N.E.T

Comments:

Incident handling relates to the handling of the critical incidents which we may feel seriously threat to the organisation. The incident co-ordinating and handling is the important and needs much improvement for performing these activities efficiently.

The improvements can be described according to various factors:

1. **General Incident Handling Considerations:**

- The nature of incident handling is very critical and it requires our deputed engineers should have expertise in handling such incidents. By having designed the course curriculum for incident handling at various level of management (i.e. at the entry level, middle level, senior level) will serve the purpose.

- Policies and procedures should be defined appropriately for handling cyber security incidents at various levels. ((I.e. at the entry level, middle level, senior level management).

- It`s good to know the proportionate of incident coverage or the percentage of number of incidents fixed or still pending to be closed or still not attended over a period of time in order to increase the efficiency of Incident handling.

- Prepare handouts on the type of incidents encountered and archive the same for the future purpose or for any future references.

- Prepare a checklist for incident management for engineering team handling incidents , to ensure the smooth operation.

- Preparing process document related to incident management for referring step by step procedure for handling incidents.

2. Organisational Capabilities and Considerations of Effective Incident Coordination:

- Define the incident handling collaboration of various hierarchies and their involvement for the same.
- Identify security measures to prevent threats from harming your network in future.
- Define the role of different organisational capabilities like IT, HR, Finance, etc in incident handling and way incidents are handled.
- It`s good to have brainstorming sessions or workshops on various topics related to Incident handling may be monthly once, so that the knowledge levels of the employees can be upgraded accordingly.
- Outline methods for recovering compromised devices on your network and mitigate the potential damage from system breaches.
- Identify the potential tools that eradicate the emerging threats.

3. Coordinated Handling of an Incident:

- The formation of incident governing body is required for taking any decisions related to incident coordination and handling events.
- It`s also required for the formation of Incident Response Team, which takes care of handling of critical incidents reported by employees.
- For the purpose of educating employees, the incident governance body can set up few awareness sessions on Cyber Security Incident Handling. The session should include the introduction to Cyber Security Incident, importance of Incident Handling, the process of Incident Handling, addressing critical incidents and conclusion.

4. Data Handling Considerations:

- List the critical data of the relevant departments which needs to be protected during incident handling and coordination activities.

- The financial impact on data should be discussed in the review meetings, if the incidents are not handled properly. The impact should be discussed at various phases of incident handling and co-ordination life cycle (i.e. at incident Identification, incident analysis, implementing solution, confirming if the incident fixed phases).

****