**Questionnaire**

*Function*: **RESPOND**

**Aswathi Ashok Kumar**

Categories: -

1. Response Planning (RS.RP)
2. Communications (RS.CO)
3. Improvements (RS.IM)

1. **Has a response plan been created to be implemented in the event of system breach?**

**Description**: Incident Response Plan refers to a documented strategy and guideline that identifies and informs appropriate personnel of their relevant duties; defines the processes that must be taken at various stages once an incident has occurred; and the tooling that must be capable of proactively taking preventive action to keep the risk from spreading across the enterprise.

Choose an item.

1. **Is your response planning adequate?**

**Description**: Response plans can be more effective when they are documented, communicated to relevant internal and external stakeholders, and regularly updated.

This can include incorporating specific scenarios in them that may be tested on a periodic basis, to allow you to review and update your response plans based on this testing.

Choose an item.

1. **Is the response plan up to date and regularly tested?**

**Description**: Response plan should be updated with latest threats and comprehensive plans for defence, critical systems and key assets, internal contact list and security protocols.

Testing the plan periodically is essential to ensure that it works effectively in real time scenarios without any problems.

Choose an item.

1. **Is there a standardised operating procedure (SOP) that is followed?**

**Description**: SOPs provide a precise sketch of the technical processes, checklists and forms to be followed by the incident response team. It can be used as an instructional tool and can be used to reduce errors. The procedures should be based on the plans and policies.

Choose an item.

1. **Is there an incident response team with clearly defined roles and responsibilities?**

**Description**: An incident response team is group of skilled professionals, within an organisation, assigned with specific roles and responsibilities. The team will perform activities such as identifying, analysing and responding immediately to an incident. An incident response team analyses information discusses observations and activities and shares important reports and communications across the company. Assigning specific roles to the members ensures timely response.

Choose an item.

1. **Do the personnel have the required skills for responding to an event?**

**Description**: Incident handling requires specialised knowledge and experience in several technical areas and its requirement might vary depending on the risk.

The members of the incident response team should have excellent technical skills, problem solving skills, critical thinking ability and good communication skills. This can lead to proper understanding of the target and responding appropriately to the incident.

Choose an item.

1. **Is the information regarding an incident shared with the external stakeholders?**

**Description**: The organisation must share the certain information regarding an incident with its external stakeholders such as ISP providers, software vendors, law enforcements etc. This proactive sharing can help in generating a threat alert to act immediately on being noticed and to seek expert advice on how to act effectively.

Choose an item.

1. **Does the policy include provisions for incident reporting?**

**Description**: The incident response team has the responsibility to report an incident to certain parties after it has been confirmed. The policies must include provision considering the reporting to what must be reported to whom, the medium and in which circumstance. Doing so ensures that individuals involved in the team take appropriate actions in responding to an event at the right time.

Choose an item.

1. **Are there documents recording past occurrences of cybersecurity events?**

**Description**: Documentation on incident identification, analysis and management process should be carefully retained and securely stored. These documents can be later used as a reference or guideline on how to approach a similar incident in future.

Choose an item.

1. **Are lessons learned meeting held periodically after the occurrence of an incident?**

**Description**: Lessons learned meeting, usually held within a few days after the incident, involves the response team and other personnel reflecting on the threats, the incident, how it occurred, what was done to intervene it and how well the intervention worked.

These meetings help the team to adopt methods to respond to a future incident and update the policies and plans for incident response.

Choose an item.

1. **Is a follow – up report created after the occurrence?**

**Description**: Creating a follow-up report for each incident is an important post-incident activity, which can be quite valuable for future use. The report provides a reference that can be used to assist in handling similar incidents. Follow-up reports should be kept for a period as specified in record retention policies.

Choose an item.

1. **Is the incident response plan reviewed frequently?**

**Description**: The point of reviewing an incident response (IR) plan is to ensure that it still addresses the real risks that an enterprise faces. Thus, reviewing the plan at least annually will ensure that the strategies to be adopted are up to date and follow the lessons learned from past occurrences.

Choose an item.

**Simran Sharma**

Categories: -

1. Analysis (RS. AN)
2. Mitigation (RS.MI)
3. Improvements (RS.IM)

1. **How well do you know what will be the impact of the incident?**  
  
Knowing the impact of the incident is important to decide the way the situation should be handled. If the impact is known it becomes easier to decide the methods which should be undertaken to overcome the situation.

2. **Are there any forensics performed?**  
  
Digital forensics is important for law enforcement and investigation. All the activities on a computer system leave a digital trace. These bits of evidences are crucial. They tell how the incident happened, who was responsible, how to respond and how to stop it from happening in future.

3.. **Incidents are categorized consistent with response plans. Do you agree**   
  
It is helpful to if the response plans are categorized with the incidents. It helps in reacting to the cyber issues.

4. **What is the process established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources?**   
  
Vulnerability Management program is important as they help in discovering the assets in your estate, detect vulnerabilities. These help the security team to act and prioritized for threats.

5. **Do you collect data from the SIEM, IDPS, Network logs, and people in the organization?**  
  
Collecting information from the SIEM, IDPS, Network logs and people because it helps in tracking down which information was leaked which lead to the cyber-attack. Keeping tracks of log can help in identifying malicious attacks. Log monitoring helps in identifying events which led to the cyber-attack

**6. Any method implemented in the company to identify the scope of the event?**  
  
If the scope of the incidents is known, it is helpful to identify to techniques to perform when a cyber issue has occurred.  
  
   
  
   
  
Mitigation Questions

1. **Is there any breach response team?**  
     
   Having a dedicated team, which is responsible for handling any cyber issue, is important. It is important because then it becomes easy to have all the information at one place as to whether there were any methods adopted by the company to handle cybercrime.
2. **Is there any individual responsible for the overall implementation of the plan?**  
     
   This is important information, so that when a cybercrime occurs, we know where to get all the details and the information of the plans which were in place.