INTERNSHIP REPORT

WEEK # 3

M. USAMA SHAHBAZ

CONTENTS

1. About The Company
2. Developing Incident Response Plans
3. Develop A Structured Approach for Responding To and Managing Security Incidents
4. Key Steps

ABOUT THE COMPANY

The **Digital Empowerment Network Pakistan** appears to be an initiative focused on improving digital literacy and empowering individuals through training and resources in areas such as cybersecurity, cloud computing, AI, and other digital technologies. These kinds of programs typically aim to bridge the digital skills gap by offering educational programs and certifications to help participants gain practical knowledge and skills that are relevant to today's job market, especially in tech-related fields.

Here's a general breakdown of what such a network could involve:

1. **Educational Programs**: Courses or training programs in areas like cybersecurity, cloud computing, AI, software quality assurance (SQA), and more.
2. **Certifications**: Certifications that help validate the skills learned during the courses, making participants more competitive in the job market.
3. **Community Development**: Initiatives to promote digital literacy in underprivileged communities, helping individuals learn how to use technology to better their lives.
4. **Networking Opportunities**: Connecting learners with professionals, mentors, and industry experts, helping them to grow their career prospects.

Since the details are based on general expectations from such networks, it's advisable to visit their official website or contact them directly to gain more specific information about their mission, vision, and services.

Create A Plan for Responding to Security Incidents

Step 1: Identifying Potential Security Incidents

- **Question for you:** What type of security threats do you think your organization or system might face? Here are a few common examples you might want to consider:
    - Phishing attacks
    - Malware (viruses, ransomware)
    - Insider threats (employees accessing information they shouldn't)
    - Data breaches (unauthorized access to sensitive information)
    - Denial of Service (DoS) attacks

Action for you:

- Write down a list of 3-5 possible security threats that you think are most relevant.

Example Input:

- **Incident Type 1:** Phishing emails to employees
- **Incident Type 2:** Malware infection from downloads
- **Incident Type 3:** Data breach due to weak passwords

Step 2: Defining Roles and Responsibilities for the Response Team

- **Question for you:** Who do you think would need to be involved in responding to a security incident in your organization? Typical roles include:
    - **Incident Response Lead:** Person in charge of managing the incident.
    - **IT Support Team:** People responsible for technical response and recovery.
    - **HR/Legal Team:** If the incident involves sensitive employee or customer data.

Action for you:

- Think about or decide on key roles in your incident response team (we can keep this general if you don't know specific names).

Example Input:

- **Role 1:** IT Specialist – Contains the threat and recovers systems
- **Role 2:** Security Analyst – Investigates the incident and monitors for further attacks
- **Role 3:** HR/Legal – Communicates with affected users and handles legal issues

Step 3: Developing Step-by-Step Response Procedures

- **Question for you:** Do you want to create a detailed response for a specific type of incident like a phishing attack? If you're unsure, we can use phishing as an example.
    - Detection: How would your system detect the incident? (e.g., email security tool flags a suspicious email)
    - Containment: How do you stop the incident from spreading? (e.g., lock compromised accounts)
    - Eradication: How do you remove the threat? (e.g., delete the phishing email from inboxes)
    - Recovery: How do you get everything back to normal? (e.g., reset passwords, notify employees)
    - Post-Incident Review: What lessons did you learn? How can you improve the response plan?

Action for you:

- Select one or more types of incidents you want to write a step-by-step response for (e.g., phishing, malware, etc.).
- I can write the procedures for you based on your input.

Example Input:

- **Incident Type:** Phishing Attack
  - Detection: IT department gets notified of a suspicious email.
  - Containment: Block the email and lock the affected user's account.
  - Eradication: Remove the email and scan the network for other signs of phishing.
  - Recovery: Reset the user's password and monitor their account.
  - Review: Investigate how the phishing email got through and improve email filters.

Step 4: Conducting Training and Simulation Exercises

- **Question for you:** How would you go about training your response team to deal with an incident?
    - **Example:** Run a phishing simulation where fake phishing emails are sent to employees to see how they respond. Then review their actions.

Action for you:

- Decide how you might simulate an attack or train your team (e.g., a mock phishing email test or security training sessions).

Example Input:

- Conduct a phishing simulation and test employees on how well they recognize and report the phishing email.

Step 5: Reviewing and Updating the Plan Regularly

- **Question for you:** How often do you think it's necessary to update the plan? Typically, plans are reviewed every 6 months or after a real incident occurs.

Action for you:

- Choose how frequently the incident response plan should be reviewed and updated.

Example Input:

- Review the incident response plan every 6 months, or after any significant security event.
