**Question**  
Pick one of the threats identified from the previous assignment: regard assets in technology, use Cybersecurity management strategies which are;

1. Identify

2. Protect

3. Detect

4. Respond

5. Recover

6. Govern

To analyze the threat.

**Answer**  
In today's rapidly advancing technology and software development industries, cybersecurity threats pose significant risks to the confidentiality, integrity, and availability of sensitive data and systems. One of the most prevalent threats is **phishing attacks**. Phishing remains a top cyber risk, targeting employees through deceptive emails or messages, ultimately attempting to steal sensitive information or gain unauthorized access to systems. In this analysis, we will examine phishing attacks using a comprehensive cybersecurity management strategy, encompassing the phases of Identify, Protect, Detect, Respond, Recover, and Govern.

### **Phishing Attacks: Cybersecurity Management Strategy Analysis**

#### **1. Identify**

* **Objective:** Recognize and assess potential phishing threats.
* **Action:** Phishing attacks can be identified by assessing the organization’s communication channels, particularly email systems, and determining the frequency and nature of attempts to deceive employees. Employees often become the primary targets for phishing, so it is essential to identify the users most vulnerable to these attacks (e.g., new employees, high-level executives, etc.).
* **Outcome:** Classifying phishing as a top security threat, identifying vulnerable assets (such as login credentials, personal data, and financial information), and evaluating the potential consequences of successful attacks.

#### **2. Protect**

* **Objective:** Implement controls to reduce the likelihood of phishing attacks and mitigate damage if they occur.
* **Action:** Employee awareness and training programs are essential, as phishing often relies on human error. Implementing multi-factor authentication (MFA), email filtering tools, and anti-phishing software are also crucial steps to mitigate the risk. Additionally, deploying strict email security protocols such as Domain-based Message Authentication, Reporting & Conformance (DMARC) can help prevent spoofed emails.
* **Outcome:** Strengthened defenses through proactive measures, reducing the likelihood of successful phishing attempts by securing communication channels and educating staff on recognizing phishing tactics.

#### **3. Detect**

* **Objective:** Monitor systems to identify phishing threats in real-time.
* **Action:** Detection involves continuous monitoring of incoming emails for suspicious activity or patterns, employing AI-based threat detection tools, and ensuring that email scanning software is regularly updated. It is also important to monitor for signs of compromised accounts or unusual behavior such as unauthorized logins or abnormal data access patterns.
* **Outcome:** Quick identification of phishing emails, allowing the security team to respond swiftly to prevent breaches.

#### **4. Respond**

* **Objective:** Take immediate action to neutralize phishing threats.
* **Action:** Once a phishing attempt is detected, the response should include isolating the compromised account, notifying the impacted user, and conducting a thorough investigation to assess any potential damage. Internal communications should be sent to warn other employees of the phishing attempt, and IT teams should block malicious IP addresses or URLs associated with the attack.
* **Outcome:** Mitigated impact of phishing attacks through timely intervention, preventing the spread of the attack to other parts of the organization.

#### **5. Recover**

* **Objective:** Restore normal operations and repair any damage caused by phishing attacks.
* **Action:** Recovery includes restoring compromised accounts and assets, resetting passwords, and ensuring that all affected systems are clean of malware or unauthorized access. This may involve collaboration with cybersecurity experts to conduct post-incident assessments and implement stronger defenses.
* **Outcome:** Full restoration of services and systems, minimizing downtime and loss, while reinforcing security against future attacks.

#### **6. Govern**

* **Objective:** Oversee the overall cybersecurity program and ensure compliance with industry standards.
* **Action:** Governance involves creating and enforcing policies, conducting regular risk assessments, and ensuring compliance with cybersecurity regulations and frameworks such as NIST or ISO 27001. Regular audits should be conducted to review the effectiveness of phishing protection strategies, and any gaps in security should be addressed through updated policies or procedures.
* **Outcome:** A well-governed cybersecurity strategy that adapts to emerging phishing tactics, ensuring continuous improvement and alignment with industry best practices.

### **Conclusion**

By leveraging the cybersecurity management strategy of Identify, Protect, Detect, Respond, Recover, and Govern, organizations can significantly reduce the risks posed by phishing attacks. Through proactive measures such as employee training, advanced detection systems, and a robust governance framework, organizations can better safeguard their assets, ensuring the protection of sensitive information and maintaining the integrity and availability of their systems.