# **Incident Report** **Template**

## **1. Executive Summary** **Task**

Summarize the report findings here and present a few key insights - **Hint: complete this last**

**Task Response**

Smart meter co Company experienced a significant cybersecurity incident resulting in the loss of sensitive and confidential data. A Phishing attack was launched against several user accounts via social engineering technique to gain unauthorized access to SCADA systems. The incident was characterized by suspicious activity, impersonation of user accounts, modification of files, deletion of files and the execution of potentially malicious processes.

The attacker gained access to the network by compromising the email server which had several unpatched vulnerabilities which lead to a phishing attack via email and subsequently a remote code execution and privilege escalation.

## **2. Incident Details**

**Task**

Describe the incident, the date and time, and severity.

**Task Response**

* **Short Description of Attack (include the attack vector and intrusion point)**:

Smart meter co Company experienced a significant cybersecurity incident resulting in the loss of sensitive and confidential data. A Phishing attack was launched against several user accounts. via social engineering technique to gain access.

**Date and Time**: 8:00am December, 2023

* **Incident Severity**: High

## **3. Root Cause Analysis**

**Tasks**

1. **Analyze the logs provided and state your high-level observations**
2. **Analyze the interview transcripts provided and state your insights from them**
3. **Then using the insights gathered from the logs and interview transcripts, complete the provided 5 Why’s analysis and the Fishbone Analysis.** 
   1. Add a screenshot of the 5 Why’s Analysis completed to identify the problem statement for the Fishbone Analysis
   2. Add a screenshot of the completed Fishbone Analysis
4. **State the identified attack vector.**
5. **State the intrusion point**

**Task Response**

**1. High Level Observations from Logs:**

**Observation 1 –**

Email server log;

The phishing email was sent from an external account claiming to be office 365 ‘’micr0soft@microsft.support.accounts.mercifulredeemerchurch.com.’’

The recipients of the phishing email were John@SmartMeterCo.com, Jack@SmartMeterCo.com, Vinod@SmartMeterCo.com, Mary@SmartMeterCo.com, [Chillantra@SmartMeterCo.com](mailto:Chillantra@SmartMeterCo.com).

8:00:25 the phishing email completed it’s transmission.

File log;

John, Vinod, and Chillantra accessed, modified, and updated files in various directories on the CriticalFileServer.

Jack accessed, copied, and attempted to update files on the CriticalFileServer., he also attempted to delete directories such as CompanyInfo, TopSectret, and HumanResources on the CriticalFileServer, but these deletion attempts failed.

**Observation 2 –**

SQL server;

Multiple actions were performed on the SmartMeterCo DB Reading table.

The updates show on Dec 15, Dec 19, and Dec 22 alter the 'Value' field in the SmartMeterCoDB Reading table in an attempt to manipulate or destroy data.

The combination of commands used indicates unauthorized access and potentially malicious activities on the database.

**2. High Level Interview Insights:**

**Insight 1 – Interview with CEO and IIOT Manager**

**Interview with CEO**

The attacker's mail to the CEO was masked as being from a familiar vendor,

which then asked for his credentials. No immediate suspicious activity was observed until days later. Yet, following the suspicious activity noticed by the CEO no action was taken to mitigate risk.

**Interview with IIOT MANAGER JOHN**

Attacker modified his approach with John, however just like the CEO no immediate suspicious activity followed. John lacked knowledge in knowing what to look out for even after he reviewed the code with irregularities.

No risk mitigation measures were taken by him as well.

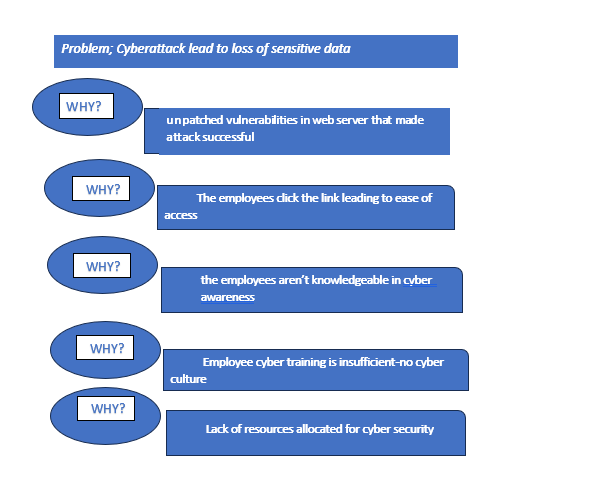
**Insight 2 – Interview with HR MANAGER CHILLANTRA**

Chillantra spotted a lot of discrepancies yet proceeded with logging in with her credentials due to the source of the mail masked as her colleague.

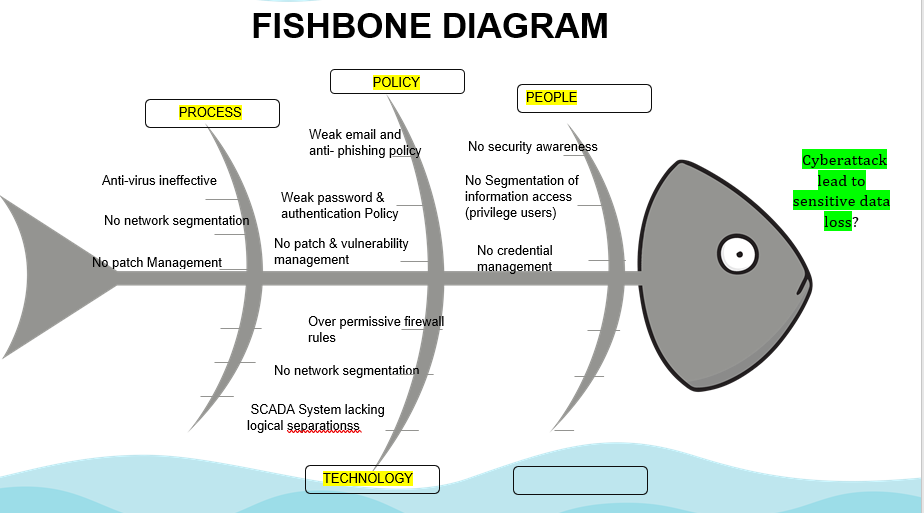
She acted on her suspicion by changing her password

**3. Root Cause Analysis Screenshots**

## **a) 5 Whys Analysis (for problem statement) screenshot**



**b) Fishbone Analysis Screenshot**



**4. Attack Vector**: Phishing, an attacker was able to successfully launch a phishing attack via social engineering technique to gain unauthorized access.

**5.** **State the intrusion point**: The attacker was able to gain access via email communication as a result of social engineering due to poor network segmentation, weak password policy and No cybersecurity awareness or culture.

## **4. Failed Controls**

**Task**

State at least 2 controls that failed further to your investigation:

**Task Response**

**Failed control 1**

Failed Control: CA-7 - Continuous Monitoring

Reason: The absence of centralized logging for antivirus activities hindered continuous monitoring capabilities, leading to a delayed detection of suspicious activities and the compromise of critical systems. System and Communications Protection (SC) Family:

**Failed control 2**

Failed Control: AT-2 - Security Awareness Training

Reason: Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining. System and Information Integrity (SI) Family:

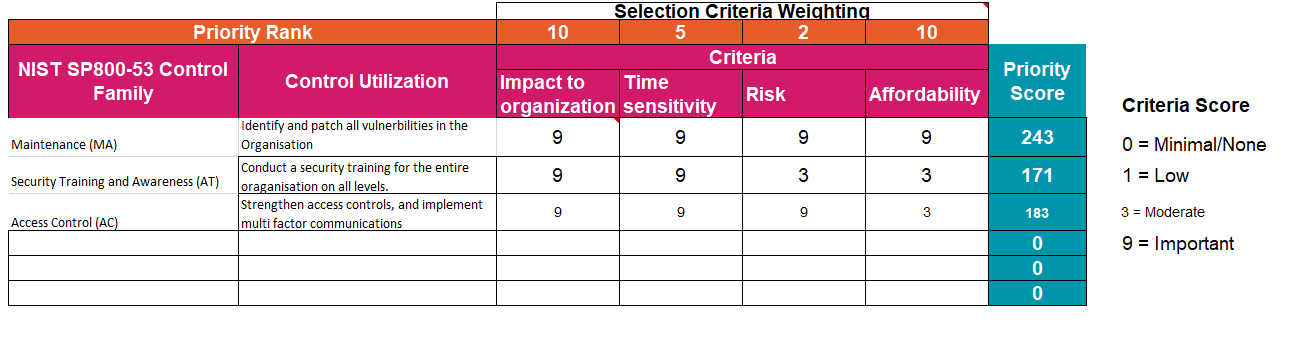
## **5. Prioritized Recommendations Based on Overall Risk**

**Tasks**

1. **Identify at least 3 recommendations to prevent such an incident from occurring again**
2. **Then, enter the identified recommendations into the prioritization template and complete the rest of the prioritization template**
3. **Add a screenshot of the completed prioritization template**

**Task Response**

**Prioritization template Screenshot**



## **6. Conclusion**

**Task**

Provide a one sentence statement on the most important recommendation to implement and why implementing it immediately is very important.

**Task Response**

It is imperative that prompt identification and addressing of any patch vulnerabilities be conducted as they present significant risks to the organization. Time is of the essence, as delaying patch updates can exacerbate the organization's vulnerability to additional attacks with different vectors. Additionally, there should be no financial burden associated with updating patches, as this should already be integrated into existing software and hardware implementations.