# **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 phishing incidents within drawing insights from interviews with key personnel: CEO Jack, IIoT Engineer John, and HR Manager Chillantra. Findings indicate a lack of awareness, reluctance to change passwords, and misplaced trust in email communications.

Immediate implementation of Centralized logging and employee Security Awareness Training is recommended to educate staff on identifying and responding to phishing attempts effectively. Additionally, deploying multi-factor authentication (MFA) and conducting regular phishing. Simulations are advised to enhance security measures and reinforce best practices.

By prioritizing these actions, we can bolster our defenses against phishing attacks, mitigate risks, and cultivate a culture of cybersecurity awareness across the organization. A Spear phishing attack which resulted in compromising user credentials of company employee which compromised user credentials, sensitive and confidential data.

## **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 employees received a phishing email that resulted in cybersecurity incident and leading to comprise sensitive information such as user credentials, intellectual property , and employee bonus on critical server . A malicious actor was able to gain unauthorized access to the Smart meter Co system and transfer some malicious files to the system.

* **Date and Time**: December 14th, 2023 and Time was 8:00 am
* **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 Logs**   
  
The email logs reveal that a phishing email was sent from "mercifulredeemerchurch.com" to the email server of Smart MeterCo. Additionally, the logs indicate that an Excel file was transferred from an external source. These activities suggest that an unauthorized user successfully gained access via a phishing email and acquired user credentials to log into the file server. Furthermore, the logs document a data command being executed to initiate changes in the SQL server, with a subsequent message confirming acceptance. Eventually, a Quit command was executed to exit the server.

**File Server Logs**   
  
The file server logs indicate that an unauthorized individual gained access to the critical file server using Smart Meterco employee credentials. This unauthorized user proceeded to tamper with sensitive information by accessing the Top-Secret files stored on the server. The logs reveal that various actions were taken, including updates to text documents such as the IOT product source code and employee Xmas bonuses. Additionally files were copied before attempting to delete. Among the folders affected were "Company Info," "Top Secret," and "Human Resources.” This shows that sensitive information may have been exposed to the unauthorized user

**Observation 2 –**

**SQL Server Logs**

The SQL server logs provide timestamps indicating the actions taken by database administrators and application users. It appears that a database admin executed a command to drop certain data, while an app user performed an action to update the data. Specifically, the timestamps indicate that meter ID readings containing "12345" digits were updated to values 100, 102, and 103, and the ID itself was changed to 54321. Subsequently changes were made by the sudo user Jack to the altered data. These logs suggest that data manipulation and deletion occurred within the SQL server environment.

**2. High Level Interview Insights:**

**Insight 1**

**Interview with CEO (Jack)**

Jack received an email from a vendor he recognized, and upon clicking the link provided in the email, he entered his user credentials. After entering his credentials, Jack observed no immediate activity, but later noticed files and emails from the SQL server and an Excel file successfully copied into his inbox. Despite this, Jack did not take any immediate preventive measures. However, he did take the initiative to forward the suspicious email to John and Vinod for further investigation.

**Insight 2**

**Interview with IoT Engineer (John)**

While John was preoccupied collaborating with Vinod on a system update, he continued to enter his credentials on a link provided in an email, believing it to be legitimate, to avoid interrupting his operations. Although he noticed some unusual changes in the code made by Jack, John attributed them to a potential initiative by the company CEO to access the IIOT platform from home. Given that John uses the same password for all accounts, he neglected to change it and was later was advised by Sarah to do so.

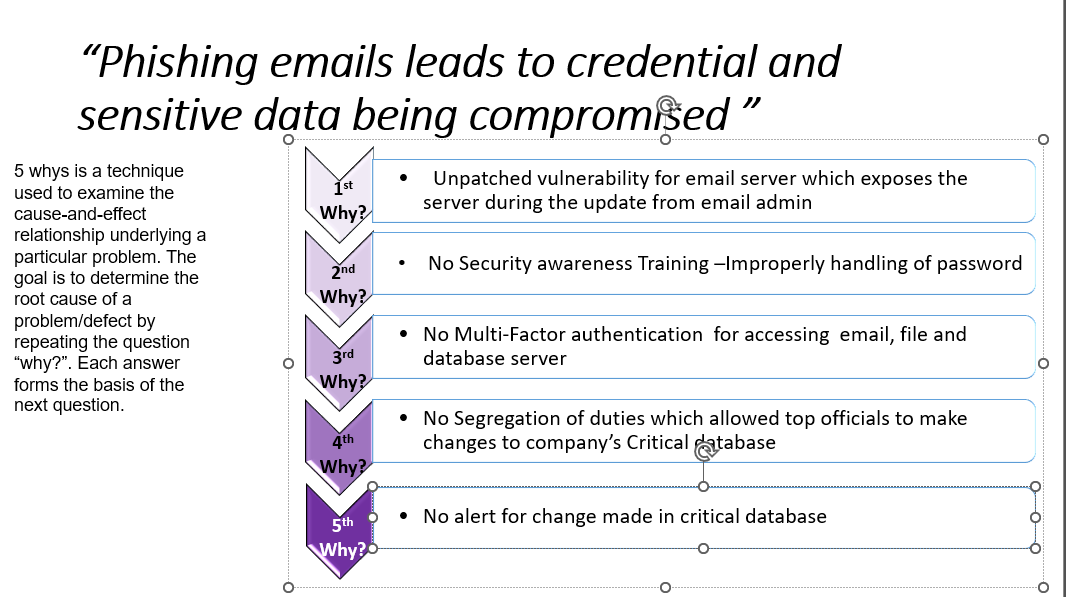
**Insight 3**

**Interview with HR Manager (Chillantra)**

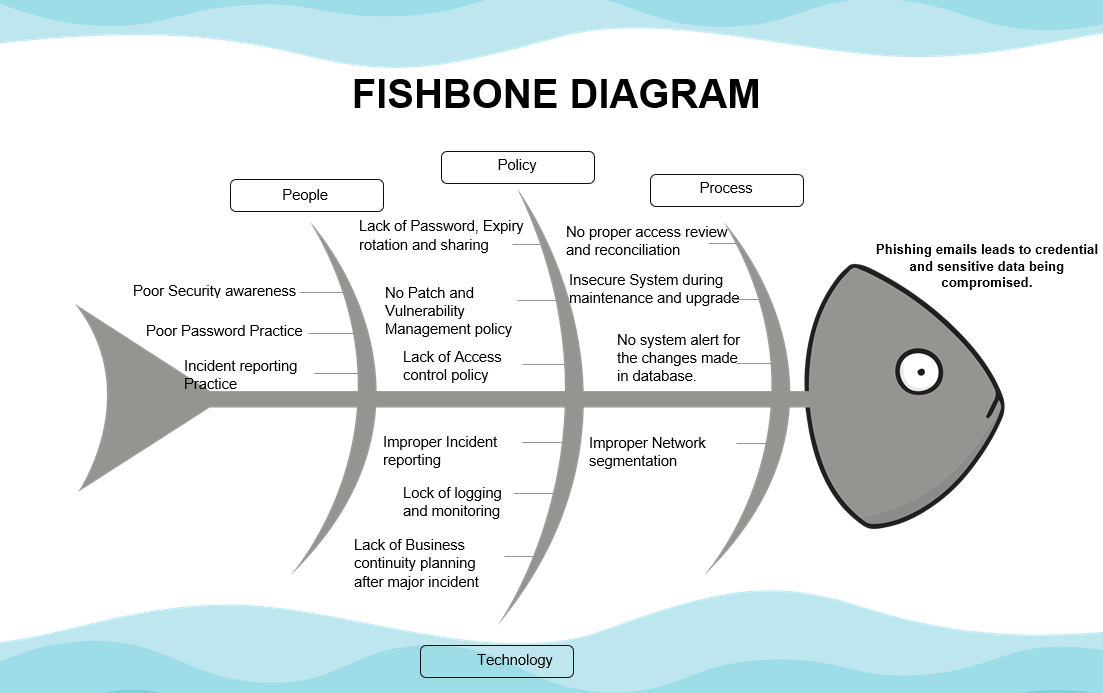
Chillantra was reviewing the email sent from John while working on Christmas bonuses, she noticed several suspicious activities. There were numerous spelling mistakes, fuzzy graphics, and the URL appeared to be unusual. Despite these red flags, Chillantra entered her credentials as the email had been forwarded from the company's CEO. However, she promptly changed her password after entering her credentials as a preventive measure.

**3. Root Cause Analysis Screenshots**

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



**b) Fishbone Analysis Screenshot**



**4. Attack Vector**: Email, an attacker was able to launch an attack by a phishing email and made changes to SQL server because of lack of segregation of duties. Since External firewall doesn’t protect email server traffic during the time of upgrading.

**5.** **State the intrusion point** : << The attacker was able to get into Critical File server and Database due to poor handling of email and lack of security practices as CEO Jack was able to access Email server through his Blackberry 630 which doesn’t have strong authentication.

## **4. Failed Controls**

**Task**

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

**Task Response**

**Failed control 1**   
  
Access control (AC) Family  
  
  
A) Failed Control AC-2 (**Account Management**)  
  
The account management was compromised primarily due to the lack of vigilance in verifying the legitimacy of emails and the reuse of passwords across multiple accounts. CEO Jack, IIoT Engineer John, and HR Manager Chillantra all fell victim to phishing emails, which led to the unauthorized disclosure of their credentials. Jack and John entered their credentials without thoroughly assessing the legitimacy of the requests, while Chillantra, despite noticing suspicious elements in the email, proceeded due to the perceived trustworthiness of the sender. Furthermore, John's reluctance to change his password, coupled with the widespread reuse of passwords, further exacerbated the security risk. Ultimately, the compromised credentials allowed unauthorized access to sensitive systems and data, highlighting the importance of robust account management practices and user awareness training.  
  
B) Failed Control AC-3(**Access Enforcement)**   
  
The account access enforcement was compromised due to the employees' failure to recognize and respond appropriately to phishing emails. The employees received emails requesting urgent verification of their credentials, leading them to enter their login information on potentially fraudulent websites. Despite noticing discrepancies such as suspicious URLs, spelling mistakes, and fuzzy graphics, they proceeded with entering their credentials due to the perceived urgency of the requests or the assumed trustworthiness of the sender. This lack of vigilance allowed unauthorized access to their accounts, highlighting the importance of robust cybersecurity awareness training and strict adherence to organizational access control policies

**C)** Failed Control AC-8**(System Use Notification)**

The system use notification failed because the employees did not receive or properly acknowledge the notification messages or banners before accessing the system. In each interview scenario, the employees clicked on links in phishing emails without encountering any system use notification messages or banners. Consequently, they were unaware of the system usage conditions, including the fact that system usage may be monitored, recorded, and subject to audit, and that unauthorized use is prohibited and subject to penalties. This failure to display and acknowledge system use notifications contributed to the success of the phishing attacks by bypassing an essential security measure meant to alert users to potential risks and responsibilities when accessing organizational systems.

**Failed Control 2  
  
A) Failed Control AT-2 (Literacy Training and Awareness)**The literacy training and awareness failed because the employees lacked the necessary knowledge and skills to recognize and respond appropriately to phishing emails. Employees failed to identify the suspicious nature of the emails, including discrepancies in the content, such as spelling mistakes, fuzzy graphics, and unusual URLs. Additionally, they did not demonstrate an understanding of the potential risks associated with entering their credentials on unfamiliar websites. Furthermore, there was a lack of reinforcement of the importance of cybersecurity hygiene, such as regularly updating passwords and reporting suspicious activities. The employees' reliance on trust in the sender, rather than critically assessing the legitimacy of the emails, indicates a gap in their understanding of cybersecurity best practices.

Overall, the failure of literacy training and awareness to effectively educate employees on recognizing and mitigating phishing threats highlights the need for more comprehensive and ongoing training, as well as practical exercises that simulate real-world scenarios to reinforce learning and enhance preparedness

## **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**

A) **Implement Centralized Logging (AU)** : Implement centralized logging to track user activities, including login attempts and access to sensitive information. This would provide better visibility into potential security incidents, such as unauthorized access due to phishing attacks.

B) **Establish Network Segmentation (SC**): Implement network segmentation to limit lateral movement of attackers within the organization's network. Dividing the network into separate segments would contain the impact of successful phishing attacks, reducing the risk of unauthorized access to critical systems and data.

C) **Enhance Boundary Protection and Firewall Rules (SC) :** Strengthen boundary protection and firewall rules to fortify the organization's perimeter defenses against external threats, including phishing attacks. This could involve implementing more robust firewall configurations and intrusion detection/prevention systems to detect and block malicious traffic before it reaches internal systems.  
  
  
  
  
A screenshot of a computer

Description automatically generated

## **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 recommended to provide Centralized logging immediately, as it poses high impact and risk to the organizations, is time sensitive as delaying updates in company’s critical servers can further compound the organization as they will safeguard company’s system against phishing attacks, enhancing compliance, and fostering a cybersecurity-conscious culture throughout our organization.