Incident Report Template

1. Executive Summary

Task

Summarize the report findings here and present a few key insights

Task Response

SmartMeter Co., a leading IIoT vendor for smart meters, experienced a significant cybersecurity incident where a phishing attack compromised the company's email server. Malicious actors gained unauthorized access to multiple user credentials, leading to a breach of the critical database and compromising sensitive and confidential data. The attack exploited the lack of employee training on identifying phishing emails and the absence of multi-factor authentication (MFA).

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)**:

  SmartMeter Co., a leading IIoT vendor for smart meters, experienced a security incident where a phishing attack targeted the company's email server by sending deceptive emails to employees, leading to the compromise of multiple user credentials. This breach allowed the malicious actor to gain unauthorized access to the critical database, further compromising sensitive and confidential data stored on SmartMeter Co.'s servers.

- **Date and Time**: 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.**
    a. Add a screenshot of the 5 Why's Analysis completed to identify the problem statement for the Fishbone Analysis
    b. 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 server logs indicate multiple incoming connections and transactions, suggesting a potential phishing attempt.

File Server Logs

The file server logs indicate multiple instances of suspicious activity involving extensive access to critical files by several users, particularly outside business hours. The patterns of repeated copying, updating, and deletion attempts suggest potential malicious activity.

Observation 2

SQL Server

The SQL Server logs reveal concerning patterns of suspicious activity and unauthorized database alterations carried out by various user accounts, like "admin," "db_admin," and "app_user." These actions include multiple instances of updating, copying, and attempting to drop the "SmartMeterCoDB.Readings" table, suggesting potential malicious intent, especially occurring outside of typical business hours. Moreover, the presence of commands for copying data to CSV files raises a concern, indicating a potential risk of data exfiltration.

2. High Level Interview Insights:

Insight 1 -

Interview with CEO(Jack):

CEO entered the credential due to it's urgent request and familiarity of the site .No necessary information or training were given to detect a phishing attempt.A few days, noticed some unusual files and emails from the SQL server being copied and some odd mails were sent from the phone.No immediate action has taken assuming it might have been carried out by one of the family members who also had accessed to the phone.

Interview with IIoT Engineer (John):

Phishing email appeared from a legitimate source, urgently requesting credential verification.Despite the discrepancies in the email, the employee entered the credentials due to multitasking. Subsequently, unexpected code updates from CEO were observed. No immediate action were taken

Insight 2

Interview with HR Manager (Chillantra):

Despite the spelling mistakes, fuzzy graphics and the URL in the email, the employee entered the credentials because the email appeared to come from a trusted colleague, which overrode the employee's initial doubts.

3. Root Cause Analysis Screenshots

a) 5 Whys Analysis (for problem statement) screenshot

5 “Whys” Template – *“Critical Data compromise”*

5 whys is a technique used to examine the cause-and-effect relationship underlying a particular problem. The goal is to determine the root cause of a problem/ defect by repeating the question “why?”. Each answer forms the basis of the next question.

1st Why?
- Attacker gained unauthorized access to critical server

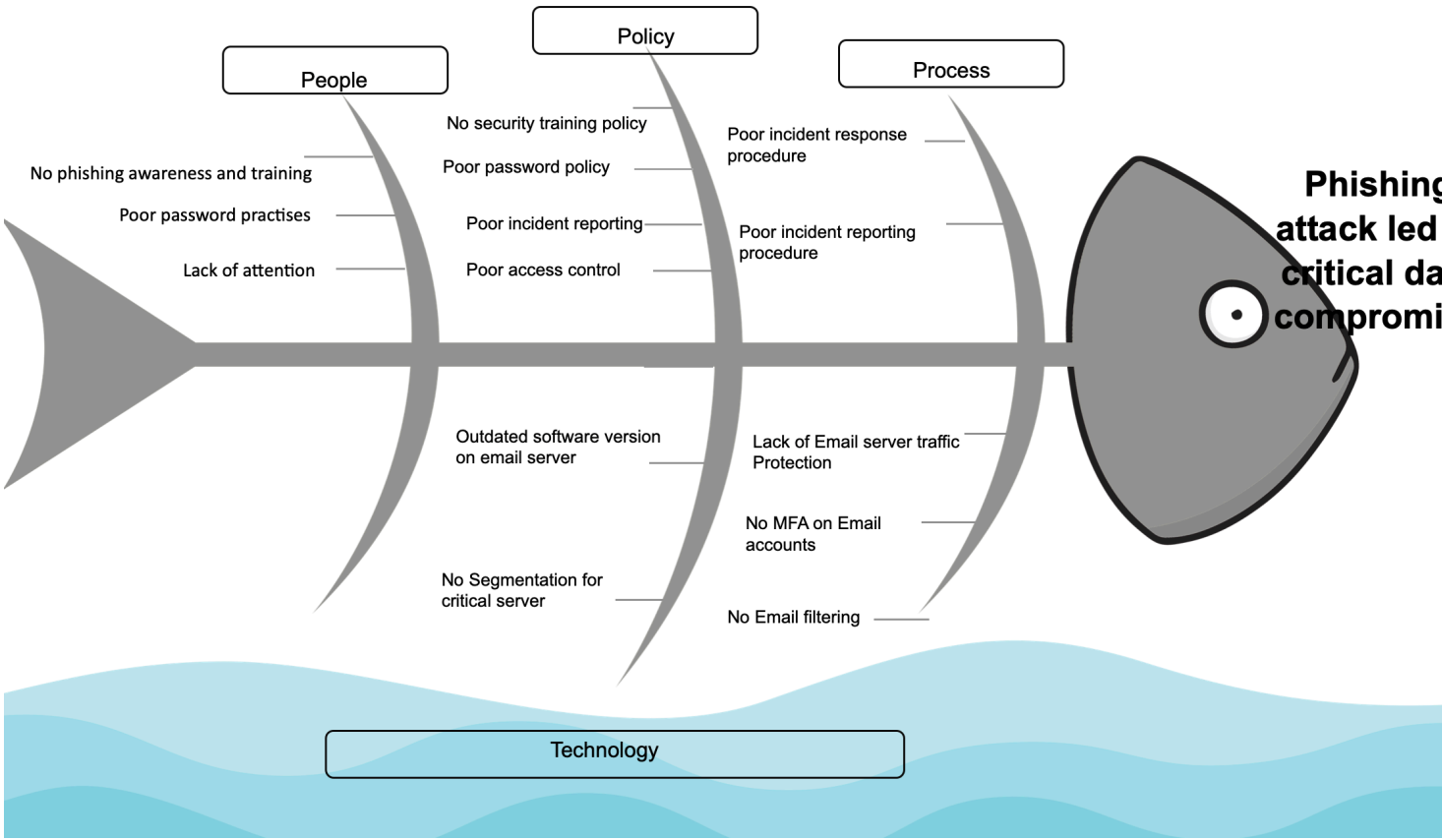
2nd Why?
- Credentials were obtained through a phishing attack

3rd Why?
- No adequate training to detect phishing ,no MFA or Segmentation

4th Why?
- lack of security awareness program and failed to implement critical security controls

5th Why?
- Prioritized operational efficiency over security

FISHBONE DIAGRAM



b) Fishbone Analysis Screenshot

4. Attack Vector: Email, attacker was able to launch a phishing attack against the company employees.

5. State the intrusion point : The attacker targeted the email server of the company by phishing.Employees entered their credentials allowing the attacker to obtain these credentials and gain unauthorized access to the email server and subsequently the critical database.

4. Failed Controls

Task

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

Task Response

Failed control 1 - Identification and Authentication Family

IA-2: Identification and Authentication - is a failed control in this scenario because employees were able to authenticate using only their credentials, which were easily captured by the phishing attack. The lack of multi-factor authentication (MFA) allowed attackers to use these compromised credentials to gain unauthorized access to critical systems without any additional verification.

Failed control 2: Awareness and training Family

AT-2: Literacy training and awareness Control - Effective literacy training and awareness would have empowered the employees to detect and respond to phishing attempts appropriately.

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

		Selection Criteria Weighting				
Priority Rank		10	5	2	10	
NIST SP800-53 Control Family	Control Utilization	Criteria				Priority Score
		Impact to organization	Time sensitivity	Risk	Affordability	
Identification and Authentication	Implement MFA	9	9	9	3	183
Awareness and Training	Conduct regular cybersecurity awareness Training	9	3	9	3	153
System And Communications Protection (SC)	Implement Email filtering	9	9	3	3	171
System And Communications Protection (SC)	Establish Network Segmentation	3	1	1	1	47
						0
						0

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 that the organization prioritize implementing multi-factor authentication (MFA) first to strengthen its security posture effectively, thereby reducing the risk of unauthorized access using compromised credentials. Following the implementation of MFA, conducting regular cybersecurity training is crucial to educate employees on recognizing and responding to phishing attacks, which pose a high impact and risk to security.