# **Incident Report**

## **1. Executive Summary**

This report investigates a security incident at SmartMeter Co. caused by a phishing attack. Several employees entered their credentials on a malicious website, leading to unauthorized access to sensitive systems, including the critical file server and SQL database. Key findings include poor password hygiene, inadequate email security controls, and a lack of phishing awareness among employees. Recommendations focus on strengthening email security, employee training, and improving access controls.

## **2. Incident Details**

* **Short Description of Attack:**  
  A phishing email campaign targeted SmartMeter Co. employees, resulting in multiple users clicking malicious links and divulging login credentials. The attacker leveraged these credentials to gain unauthorized access to sensitive data stored on internal servers, exploiting weak access controls and a lack of multi-factor authentication (MFA).
* **Date and Time:** The incident occurred on December 14, 2023, and escalated over subsequent days.
* **Incident Severity:** High - sensitive intellectual property and customer data were exposed.

## **3. Root Cause Analysis**

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

**Observation 1 -** Logs from the email server show phishing emails sent to multiple employees (e.g., Jack, John, Vinod) containing an external link that led to credential theft. The email headers indicate the spoofed sender address mimicked a trusted domain, tricking recipients into believing the email was legitimate. Recipients interacted with the link, which redirected them to a fake login page designed to harvest their credentials.

**Observation 2 -** File server logs reveal unauthorized access and copying of sensitive files, including the IIoT product source code and employee information. Specifically, users John and Vinod accessed and updated critical files within hours of the phishing attack. These activities suggest that their compromised accounts were used to exfiltrate sensitive intellectual property and modify key documents. Additionally, unsuccessful deletion attempts were logged, indicating potential cover-up actions by the attackers.

**2. High Level Interview Insights:**

**Insight 1 -** Jack (CEO) entered his credentials on the phishing site after receiving an urgent email that appeared to be from a trusted vendor. He noted the email’s familiarity and urgency influenced his decision to comply without verifying the sender’s authenticity. Jack also shared the email with John and Vinod for further review, inadvertently expanding the compro

**Insight 2 -** John (IIoT Engineer) admitted to frequently entering credentials for similar emails due to his need for seamless access to systems. He was multitasking during the incident, which reduced his ability to detect the phishing attempt. He also forwarded the phishing email to other employees, including Chillantra, amplifying the attack’s impact.

**Insight 3 -** Chillantra (HR Manager) recognized some red flags in the email, such as spelling mistakes and an unfamiliar URL. However, she proceeded to enter her credentials because the email came from John, whom she trusted. Her decision highlights the risks posed by social engineering and internal trust exploitation.

**3. Root Cause Analysis**

## **a) 5 Whys Analysis**

1. Why did attackers gain access? Employees entered credentials on a phishing site.
2. Why did employees enter credentials? Lack of phishing awareness.
3. Why was there a lack of awareness? Insufficient training on email threats.
4. Why was training insufficient? No formal program addressing social engineering.
5. Why was there no program? Cybersecurity awareness was not prioritized

**b) Fishbone Analysis**

A diagram of a fish

Description automatically generated

**4. Attack Vector**: Phishing emails containing links to a spoofed login page that mimicked a trusted vendor’s platform. The attackers used social engineering tactics, leveraging urgency and familiarity to deceive recipients into providing their credentials.

**5.** **State the intrusion point:** The intrusion point was the employees’ compromised credentials. These credentials granted attackers access to internal systems, including the email server, critical file server, and SQL database. Exploiting these points, attackers retrieved sensitive data and attempted unauthorized actions.

## **4. Failed Controls**

**Failed control 1 –** NIST SP 800-53 Rev. 5: **SI- 4 System monitoring**

Email filtering mechanisms failed to block phishing emails containing suspicious links. The system lacked advanced heuristics or pattern recognition to identify and quarantine deceptive emails

**Failed control 2 –** NIST SP 800-53 Rev. 5: **IA- 2 Identification and Authentication**

Weak authentication protocols allowed attackers to access systems using stolen credentials. The lack of multi-factor authentication (MFA) left critical systems vulnerable to compromise once login credentials were obtained.

**Failed control 3 –** NIST SP 800-53 Rev. 5: **AT-2: Security Awareness Training**

User awareness training was inadequate, leading to employees failing to recognize phishing attempts. Employees trusted suspicious emails based on internal familiarity and urgency, revealing a gap in social engineering defenses.

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

**Implement Multi-Factor Authentication (MFA)**

Enforce MFA across all systems to ensure that credentials alone are insufficient for access. This provides an additional security layer, requiring verification through secondary methods such as mobile authentication apps or hardware tokens. MFA reduces the likelihood of unauthorized access even if credentials are compromised.

**Conduct Regular Phishing Awareness Training**

Implement a comprehensive and continuous training program to educate employees about recognizing and responding to phishing attempts. Simulated phishing exercises can enhance preparedness.

**Deploy Advanced Email Filtering Solutions:**

Upgrade email filtering systems to include heuristic and AI-based detection of phishing emails. Employ sandboxing technologies to isolate and analyze suspicious attachments and links before they reach end-users.

A screenshot of a computer

Description automatically generated

## **6. Conclusion**

The most critical recommendation is to implement multi-factor authentication (MFA) immediately to prevent unauthorized access, even if credentials are compromised. MFA significantly reduces the risk of similar incidents, providing a robust foundation for security improvements.