Cybersecurity Incident Report: Unauthorized Access Incident Analysis

1. Executive Summary

- **Incident Description:**
  This morning, an intern reported being unable to log into her internal network account. However, access logs show that her account had recently accessed customer database records. The intern mentioned receiving an email this morning requesting that she visit an external website to log in with her internal network credentials to retrieve a message. We suspect that this phishing attempt allowed a malicious actor to gain access to our network and customer database. Additionally, several employees have reported missing or altered customer records, suggesting data manipulation.

2. Identification Phase

- **Action Taken:**
  The incident management team conducted a full audit of the affected systems, devices, and access policies. The team discovered that a malicious actor obtained the intern's username and password and used them to access customer database records. The initial review confirmed that some customer data had been deleted from the database.
- **Initial Impact:**
  Some customer data was compromised, deleted, or altered. This poses a significant risk to data confidentiality and integrity.

3. Protection Phase

- **Actions Implemented:**
  1. Multi-Factor Authentication (MFA):
     MFA has been implemented to strengthen internal network access security.
  2. Login Attempt Limitation:
     Login attempts are now limited to three failed attempts to prevent brute-force attacks.
  3. Employee Training:
     Mandatory training has been initiated for all employees on securing login credentials, particularly against phishing attacks.

4. Enhanced Security Infrastructure:
   A more robust firewall has been implemented, and plans are in place to install an Intrusion Prevention System (IPS) to detect and block intrusion attempts.

4. Detection Phase

- **Continuous Monitoring:**
  - The team has deployed an Intrusion Detection System (IDS) to monitor all incoming network traffic and detect suspicious behavior in real-time.
  - Advanced logging tools will be used to continuously audit network access and monitor for any anomalous activity.

5. Response Phase

- **Immediate Actions:**
  1. Account Deactivation:
     The compromised intern's account has been deactivated immediately to prevent further unauthorized access.
  2. Management and Client Notification:
     Senior management has been notified of the incident and will reach out to affected clients via email to inform them of the data breach.
  3. Reporting to Authorities:
     In accordance with local regulations, the incident will be reported to relevant authorities and regulatory organizations.

6. Recovery Phase

- **Data Restoration:**
  - Deleted customer data will be restored using the full backup of the database from the previous night. All staff have been informed that any customer information entered or modified this morning will need to be re-entered once the restoration process is complete.
  - A validation process has been set up to ensure data integrity post-restoration and to verify that no critical information is missing.

7. Recommendations and Lessons Learned

- Strengthening Authentication:
  Multi-factor authentication and ongoing training are essential to preventing future incidents.
- Enforcing Stricter Security Policies:
  Restricting access to critical information through stricter controls and regular access audits.
- Improved Communication and Awareness:
  Employees must be more vigilant and report suspicious emails immediately to reduce phishing risks.