RISK ASSESSMENT: DATA BREACH IN A MULTINATIONAL RETAIL CORPORATION DUE TO PHISHING ATTACK

Executive Summary: As a Risk Management Officer at a multinational retail corporation, I led a Data Breach Risk Assessment following a phishing attack that compromised employee credentials and exposed sensitive customer data. By applying risk identification, assessment, and mitigation techniques, I evaluated the breach's impact and implemented corrective measures to strengthen security, enhance employee awareness, and safeguard sensitive information, ensuring the company was better prepared for future threats. The steps taken can be seen below:

1. **Risk Identification**

- **Risk Description**: Unauthorized access to a customer database containing sensitive personal information (e.g., names, addresses, credit card numbers) due to a successful phishing attack. The attack led to compromised employee credentials, allowing unauthorized access.
- **Threat Source**: Cybercriminals conducting phishing attacks to steal employee credentials.
- **Vulnerabilities**:
    - Lack of employee awareness and training on phishing threats.
    - Insufficient email filtering and phishing detection mechanisms.
    - Inadequate multi-factor authentication (MFA) implementation.
    - Poor incident response and monitoring processes.
- **Assets at Risk**:
    - Customer personal data (names, addresses, credit card numbers).
    - Company's reputation and customer trust.
    - Legal and regulatory compliance status.

2. **Risk Assessment**

- **Likelihood of Occurrence**: **High**
    - Phishing attacks are common, and the successful compromise suggests that existing defences are inadequate.
- **Impact Assessment**: **Severe**
    - **Financial Impact**: Costs associated with breach notifications, credit monitoring for affected customers, potential fines, and legal fees.
    - **Reputational Impact**: Loss of customer trust, potential customer churn, and damage to the brand.
    - **Operational Impact**: Resources diverted to incident response, recovery, and remediation.

    - **Regulatory Impact**: Potential penalties for non-compliance with data protection regulations (e.g., GDPR, CCPA).

- **Overall Risk Rating**: **Critical**
    - Given the high likelihood and severe impact, this risk is considered critical and requires immediate attention.

3. **Risk Mitigation**

- **Preventive Controls**:
    - **Employee Training**: Implement regular phishing awareness training programs to educate employees on recognizing and responding to phishing attempts.
    - **Email Security**: Deploy advanced email filtering solutions with phishing detection and prevention capabilities.
    - **Multi-Factor Authentication (MFA)**: Enforce MFA across all employee accounts to add an additional layer of security against credential theft.
    - **Least Privilege Access**: Restrict access to sensitive data to only those employees who need it to perform their job functions.
- **Detective Controls**:
    - **Continuous Monitoring**: Implement continuous monitoring solutions to detect and respond to suspicious activity in real-time.
    - **Incident Detection**: Improve the ability to detect compromised credentials through threat intelligence and behaviour analysis tools.
- **Corrective Controls**:
    - **Incident Response Plan**: Strengthen the incident response plan to ensure timely and effective response to data breaches.
    - **Breach Notification**: Develop a breach notification protocol in compliance with regulatory requirements to inform affected customers promptly.
    - **Post-Incident Review**: Conduct a thorough post-incident review to identify gaps in security and implement improvements.
- **Residual Risk**:
    - After implementing the above controls, the residual risk should be reassessed. While these measures significantly reduce the likelihood and impact, the organization must continually monitor and adjust controls as threats evolve.

4. **Risk Monitoring and Review**

- **Regular Audits**: Perform regular security audits and risk assessments to ensure the effectiveness of implemented controls.
- **Update Policies**: Continuously update security policies and procedures to reflect the latest best practices and regulatory requirements.

- **Continuous Improvement**: Implement a continuous improvement process for security measures, incorporating lessons learned from incidents and evolving threats.

This assessment highlighted the critical nature of the data breach risk posed by a phishing attack and provided a structured approach to effectively mitigate, monitor, and respond to similar risks in the future.