CYBERSECURITY BREACH ANALYSIS QUESTIONNAIRE

For Comprehensive Data Collection and Analysis

Student: 190444041 Murat KUZUCU

Course: CENG 418

Created: May 16, 2025

CYBERSECURITY BREACH ANALYSIS QUESTIONNAIRE

1. BASIC INFORMATION

1.1. Organization/Company Name:

____

1.2. Country:

____

1.3. Year of Breach:

____

1.4. Industry Sector:

[ ] Finance [ ] Healthcare [ ] Retail

[ ] Technology [ ] Manufacturing [ ] Education

[ ] Government [ ] Energy [ ] Telecommunications

[ ] Other

1.5. Organization Size:

[ ] Small (<50 employees) [ ] Medium (50-250 employees)

[ ] Large (251-1000 employees) [ ] Enterprise (>1000 employees)

CYBERSECURITY BREACH ANALYSIS QUESTIONNAIRE

2. ATTACK DETAILS

2.1. Attack Type (Select all that apply):

[ ] Ransomware

[ ] Phishing

[ ] Man-in-the-Middle

[ ] Password Attack

[ ] Zero-day Exploit

[ ] Business Email Compromise

[ ] DDoS

[ ] SQL Injection

[ ] Malware

[ ] Cross-site Scripting

[ ] Insider Threat

[ ] Other

2.2. Attack Source:

[ ] State-Sponsored Actors

[ ] Organized Crime

[ ] Insider Threat

[ ] Other

[ ] Hacktivists

[ ] Independent Hackers

[ ] Unknown

2.3. Security Vulnerability Type:

[ ] Software Vulnerability

[ ] Configuration Error

[ ] Outdated Systems

[ ] Lack of Encryption

[ ] Other

[ ] Hardware Vulnerability

[ ] Social Engineering

[ ] Weak Authentication

[ ] Missing Patches

CYBERSECURITY BREACH ANALYSIS QUESTIONNAIRE

3. IMPACT ANALYSIS

3.1. Financial Loss (in Million $):

[ ] <1
[ ] 1-5
[ ] 5-10
[ ] 10-50
[ ] 50-100
[ ] >100
[ ] Unknown

3.2. Number of Affected Users:

[ ] <1,000
[ ] 1,000-10,000
[ ] 10,000-100,000
[ ] 100,000-1,000,000
[ ] >1,000,000
[ ] Unknown

3.3. Financial Impact Category:

[ ] Low
[ ] Medium
[ ] High
[ ] Critical
[ ] Not Applicable

3.4. Type of Data Compromised (Select all that apply):

[ ] Personal Information (PII)
[ ] Payment Card Information
[ ] Health Information
[ ] Intellectual Property
[ ] Authentication Credentials
[ ] Confidential Information
[ ] Email Content
[ ] Customer Records
[ ] Other

CYBERSECURITY BREACH ANALYSIS QUESTIONNAIRE

4. INCIDENT RESPONSE AND RESOLUTION

4.1. Defense Mechanism Used:

[ ] AI-Based Threat Detection

[ ] Firewall

[ ] DDoS Protection

[ ] Access Control

[ ] Data Encryption

[ ] EDR Solution

[ ] SIEM System

[ ] Multi-factor Authentication

[ ] Intrusion Prevention

[ ] Endpoint Protection

[ ] Other

4.2. Incident Resolution Time (Hours):

[ ] <24

[ ] 24-48

[ ] 48-72

[ ] 72-168

[ ] >168

[ ] Ongoing

4.3. Detection Time Category:

[ ] Immediate (minutes)

[ ] Quick (hours)

[ ] Medium (days)

[ ] Late (weeks)

[ ] Very Late (months)

[ ] Unknown

4.4. Detection Method:

[ ] Internal Security Team

[ ] Security Product Alert

[ ] External Notification

[ ] Anomaly Detection

[ ] Routine Audit

[ ] User Report

[ ] Third-Party Security Service

[ ] Other

CYBERSECURITY BREACH ANALYSIS QUESTIONNAIRE

5. SECURITY POSTURE AND INFRASTRUCTURE

5.1. Security Posture Assessment:

[ ] Basic [ ] Intermediate [ ] Advanced [ ] Leading

5.2. Cloud Adoption Level:

[ ] None [ ] Minimal [ ] Moderate [ ] High [ ] Full Cloud

5.3. Security Measures in Place Before the Incident:

[ ] Regular Security Assessments [ ] Penetration Testing

[ ] Employee Security Training [ ] Incident Response Plan

[ ] Data Backup Strategy [ ] Patch Management Process

[ ] Network Segmentation [ ] Access Control Policies

[ ] Other

CYBERSECURITY BREACH ANALYSIS QUESTIONNAIRE

6. ADDITIONAL INFORMATION

6.1. Please describe key lessons learned from this incident:

6.2. Please describe any additional details about the incident:

CYBERSECURITY BREACH ANALYSIS QUESTIONNAIRE

CONFIRMATION

I confirm that all information provided in this questionnaire is accurate and complete to the best of my knowledge. I understand that this information will be used for cybersecurity analysis purposes.

Prepared by:

Student ID: 190444041

Name: Murat KUZUCU

Course: CENG 418

Date:

Signature: