MODERN CYBERSECURITY BREACH ANALYSIS - UPDATED QUESTIONNAIRE

This questionnaire has been updated to match the enhanced dataset structure

SECTION 1: ORGANIZATION PROFILE

1. What industry does your organization primarily operate in?
- Banking/Finance/FinTech
- Healthcare/Medical Devices
- Education/EdTech
- Retail/E-commerce
- IT/Technology/SaaS
- Government/Public Sector
- Telecommunications/ISP
- Other (please specify): _____

2. What is the approximate size of your organization?
- Small (1-50 employees)
- Medium (51-500 employees)
- Large (501-5000 employees)
- Enterprise (5000+ employees)

3. What is your organization's cloud adoption level?
- On-premises
- Hybrid
- Cloud-native
- Multi-cloud

SECTION 2: SECURITY BREACH EXPERIENCE

4. What type of attack did your organization experience?
- Phishing/Spear-phishing/Business Email Compromise
- Ransomware/Double-extortion ransomware
- DDoS
- SQL Injection/Web application attacks
- Malware/Advanced Persistent Threat
- Man-in-the-Middle/Credential Interception
- Other (please specify): _____

5. What was the approximate total financial impact from the breach? (in USD)
- Less than $10,000
- $10,000 - $50,000
- $50,001 - $100,000
- $100,001 - $500,000
- $500,001 - $1 million
- $1 million - $5 million
- $5 million - $10 million
- More than $10 million
- Unknown/Still calculating

6. How many users/records were affected by this breach?
- Less than 100
- 100 - 1,000

■ 1,001 - 10,000
■ 10,001 - 100,000
■ 100,001 - 1 million
■ More than 1 million
■ Unknown

7. What was the approximate time to detect the breach?

■ Less than 24 hours
■ 1-7 days
■ 1-4 weeks
■ 1-3 months
■ 3-6 months
■ More than 6 months
■ Unknown/Still investigating

8. What was the approximate time to resolve the breach?

■ Less than 24 hours
■ 1-3 days
■ 4-7 days
■ 1-2 weeks
■ 2-4 weeks
■ 1-3 months
■ More than 3 months

9. What were the primary security vulnerabilities that led to the breach?

■ Unpatched Software
■ Weak Passwords
■ Social Engineering
■ Zero-day
■ Other (please specify): _____