**Data Breach Trends**

1. **In your professional experience, what is the most common cause of data breaches in the industries you specialize in?**
   * A) Phishing attacks
   * B) Insider threats
   * C) Misconfigured systems
   * D) Weak or stolen credentials
   * E) Other
2. **How frequently do organizations under your expertise report data breaches?**
   * A) Weekly
   * B) Monthly
   * C) Quarterly
   * D) Annually
   * E) Rarely
3. **What type of data is most commonly targeted in breaches you’ve investigated?**
   * A) Personal Identifiable Information (PII)
   * B) Financial data
   * C) Intellectual property
   * D) Healthcare records
   * E) Other

**Data Breach Prevention**

1. **Which security measure do you find most effective in preventing data breaches?**
   * A) Regular security audits
   * B) Multi-factor authentication (MFA)
   * C) Encryption of sensitive data
   * D) Continuous monitoring and detection systems
   * E) Other
2. **In your professional opinion, how effective are organizations at identifying breaches in their early stages?**
   * A) Very effective
   * B) Moderately effective
   * C) Somewhat effective
   * D) Ineffective
   * E) Other

**Breach Impact and Response**

1. **What do you observe as the biggest consequence of data breaches for organizations?**
   * A) Financial loss
   * B) Reputational damage
   * C) Regulatory fines
   * D) Loss of customer trust
   * E) Other
2. **How prepared are organizations to respond effectively to a major data breach?**
   * A) Very prepared
   * B) Moderately prepared
   * C) Somewhat prepared
   * D) Not prepared

**Specialist Insights**

1. **What area should organizations invest in most to reduce the risk of data breaches?**
   * A) Employee training on cybersecurity awareness
   * B) Advanced threat detection tools
   * C) Incident response planning
   * D) Regular vulnerability assessments and penetration testing
   * E) Other

\*check box