9 Steps to Success with Risk-Adaptive Data Protection

1. Begin with a comprehensive risk assessment:
   - Choose a methodology (e.g., CBA, BIA) and engage stakeholders.
   - Prioritize risks (1-5) based on impact and likelihood.
   - Define an acceptable response time for various severity levels.

2. Create a Data Incident Severity and Response Chart:
   - Visualize risk levels and response times.
   - Adjust priorities as needed.

3. Set up a baseline monitoring period:
   - Establish a 30-day baseline for monitoring.
   - Compare current data flows against baseline.

4. Monitor and risk reduction:
   - Regularly compare data flows.
   - Adjust risk levels as necessary.

5. Establish an Incident Management Process:
   - Automate incident response.
   - Enable quick resolution.

6. Automate policy enforcement:
   - Implement risk-adaptive policies.
   - Block, restrict or audit data based on risk.

7. Audit & Notify:
   - Monitor data flows continuously.
   - Provide notifications when policy enforcement is applicable.

8. Increase data protection program stability, scalability, and operational efficiency:
   - Automate policies across endpoints, cloud.
   - Enhance protection with risk-adaptive data protection.

9. Move to proactive protection:
   - Introduce real-time coaching.
   - Offer training to employees as needed.
   - Present findings to executive team.

For more information on implementing risk-adaptive data protection, visit www.forcepoint.com.