9 Steps to Success with Data Protection

1. Discover Data from Risk to Action
   - Identify, inventory, and risk-profile your organization's data to understand its risk level and potential impact.
   - Assemble a data protection team and determine who will drive your initiatives forward.

2. A Risk-adaptive Solution
   - A risk-adaptive solution lets you analyze incidents based on individual risk level, without needing to engage an incident response team.
   - The Risk-adaptive Difference: versus incidents requiring investigation with graduated enforcement. The summary should show the number of incidents for each risk level 1-5, contrasted against those actually requiring investigation (risk levels 4-5).

3. Create a Data Incident Severity and Response Chart
   - On a scale of 1-5 (1=low impact, 5=high impact) and define an acceptable response time for each according to the severity of the risk.
   - Use automated policy enforcement to ensure that controls are enforced based on risk level.

4. Initiate a Data Baseline
   - Monitor the behavior you've observed and set a baseline to help you recognize normal user behavior.
   - Identify the high-risk activity to focus where they're most effective.

5. Move to Proactive Protection
   - Once you have your network data protection solution in place, begin to pass the torch by having the security team host a kickoff meeting.
   - Begin to pass the torch by having the security team host a kickoff meeting.

6. Know the Fast Lane
   - In order for your team to respond quickly, it is essential to have the appropriate teams in place.
   - Consider offering real-time coaching to reinforce those processes.

7. Organize Your Data
   - Ensure that your data is organized in such a way that it can be easily accessed and protected.
   - Use incident response to get them comfortable with your processes. You might also consider offering real-time coaching to reinforce those processes.

8. Identify the Critical Response Teams
   - Consider having critical response teams in place.
   - Assign key roles such as technical administrators, incident analysts, forensics investigators, and auditors and bestow the proper rights and access to each.

9. Protect or Perish
   - Remember, the aim of data protection is to keep your data safe and provide an acceptable response time for each according to the severity of the risk.
   - Use automated policy enforcement to ensure that controls are enforced based on risk level.

Your executive team, along with recommendations for how to mitigate risks. You can then put those recommendations into action, monitor their success, and present to your executive team.