9 Steps to Success with Data Protection

1. Start with a data classification
   - Define data types and categorize them based on their importance and sensitivity.

2. Select a risk-adaptive solution
   - Choose a solution that automatically enforces policies based on risk level, reducing the need for manual intervention.

3. Implement a change model
   - Transition departmental teams into a new way of operating, with support from key stakeholders.

4. Prepare an incident response plan
   - Establish clear procedures for identifying, analyzing, and resolving data breaches efficiently.

5. Get your team involved
   - Involve key stakeholders in the process to ensure buy-in and effective implementation.

6. Automate what's possible
   - Automate routine tasks to save time and reduce the risk of human error.

7. Review and refine
   - Regularly review the effectiveness of your data protection controls and make adjustments as necessary.

8. Monitor and report
   - Use analytics to monitor data usage and identify potential risks in real-time.

9. Enhance user education
   - Continuously educate users on data protection best practices to prevent breaches from occurring.

**Priority of Incident**

| Level 1 | Low |
| Level 2 | Medium |
| Level 3 | High |

**Channels**

- FTP
- Email
- IM
- HR
- Compliance
- SSL Inspection
- Encryption
- Web
- Web

**Additional Granularity**

- Automated policy enforcement
- Audit
- Restrict/Notify/Quarantine
- Audit
- Notify

**Goals**

- 50%+ reduction
- 90%+ reduction
- 100% reduction

**Network Segments**

- Network
- Printer
- Internal  Audit
- Low/Medium
- Medium
- High

**Data Protection**

- Data types: sensitive, confidential, proprietary.
- Policies: access controls, encryption, auditing.
- Technologies: firewalls, intrusion detection systems, data loss prevention tools.

**Incident Response**

- Immediate response to critical incidents, escalating as necessary.
- Long-term strategies to prevent future incidents.

**Actions**

- Analyze data usage patterns to identify anomalies.
- Implement controls to mitigate risks.
- Continuously monitor and update policies and technologies.