DATA SECURITY CHEAT SHEET
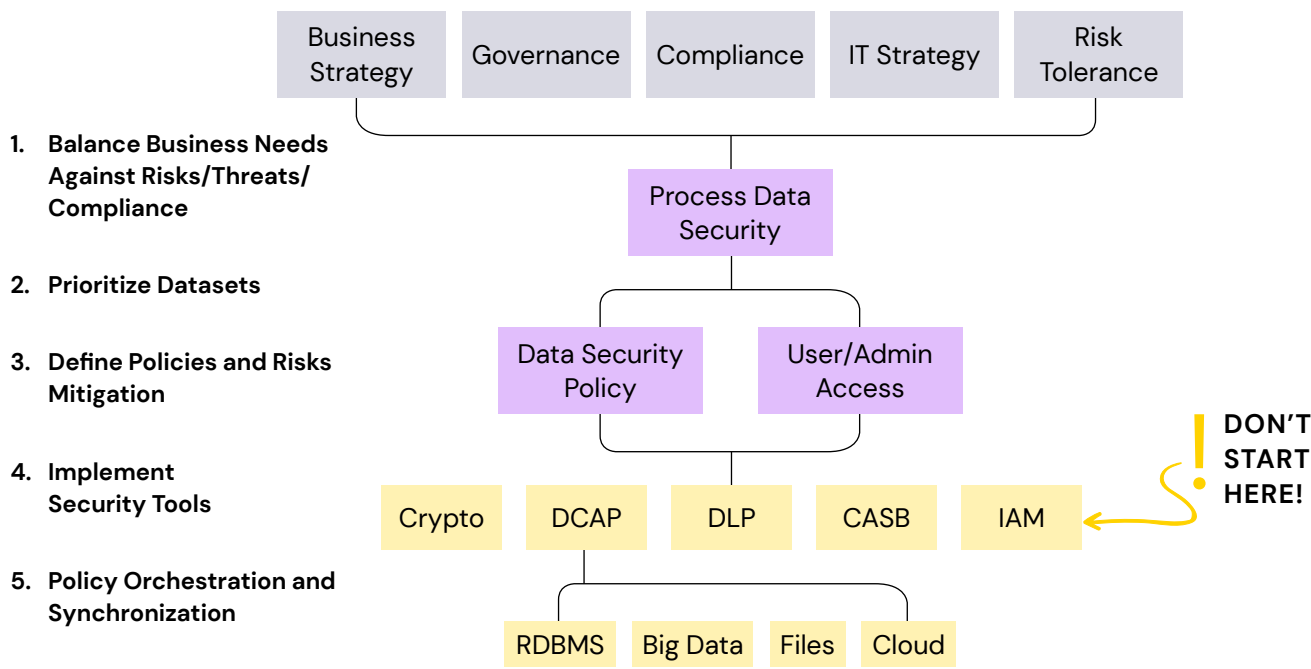
by Sergey Gromov

Your Data Guy

DEVELOP DATA SECURITY GOVERNANCE TO STOP ALL BREACHES

Business Strategy | Governance | Compliance | IT Strategy | Risk Tolerance

Process Data Security

Data Security Policy | User/Admin Access

Crypto | DCAP | DLP | CASB | IAM

RDBMS | Big Data | Files | Cloud

! DON'T START HERE!

1. **Balance Business Needs Against Risks/Threats/Compliance**

2. **Prioritize Datasets**

3. **Define Policies and Risks Mitigation**

4. **Implement Security Tools**

5. **Policy Orchestration and Synchronization**

SOFTWARE PRODUCTS FOR DATA SECURITY

1 ENCRYPTION AND KEY MANAGEMENT
Symmetric and Asymmetric Encryption Algorithms.
Key Management Solutions (e.g., AWS Key Management Service, Azure Key Vault)

2 DATA LOSS PREVENTION (DLP)
DLP Solutions (e.g., Symantec DLP, McAfee DLP, Forcepoint DLP)

3 SECURITY MONITORING AND AUDITING
Security Information and Event Management (SIEM) Tools (e.g., Splunk, IBM QRadar)

4 DATA MASKING AND ANONYMIZATION
Data Masking Solutions (e.g., Delphix, Informatica Dynamic Data Masking)

DATA SECURITY ASSESSMENT

✓ Evaluate existing data security measures and vulnerabilities.

✓ Identify potential risks and threats to data security.

✓ Assess regulatory and compliance requirements.

TEAMS NEEDED TO SUPPORT DATA SECURITY

DATA SECURITY TEAM
- Chief Information Security Officer (CISO) or Security Manager
- Security Analysts
- Security Engineers
- Incident Response Team

DATA GOVERNANCE TEAM
- Data Governance Manager
- Data Stewards
- Compliance Officers

IT OPERATIONS TEAM
- System Administrators
- Network Administrators
- Database Administrators

DATA PROTECTION CORE PRINCIPLES

Openness — Organisations must be open about personal data practices

Collection limitation — Collection of personal data must be limited, lawful and fair

Purpose specification — Purpose of collection and disclosure must be specified

Use limitation — Use of data must be limited to specific purposes

Security — Personal data must be subject to appropriate safeguards

Data quality — Personal data must be relevant, accurate and up-to-date

Access and correction — People must be able to access and correct their personal data

Accountability — Data controllers must comply with the data protection principles

KPIs FOR PERFORMANCE EVALUATION

DATA SECURITY
Number of security incidents/breaches.
Mean Time to Detect (MTTD) security incidents.
Mean Time to Respond (MTTR) to security incidents.
Percentage of data encryption coverage

DATA COMPLIANCE
Compliance with data security regulations (e.g., GDPR, HIPAA).
Number of compliance violations or incidents

EMPLOYEE AWARENESS
Completion rate of data security training.
Number of reported security incidents by employees

INCIDENT RESPONSE
Time taken to identify and contain security incidents.
Time taken to recover from security incidents.
Effectiveness of incident response processes (post-incident analysis)

Follow **@gromovsergey** for Data, Analysis & Modern technologies insights!

DATA MIND   https://datamindus.com