The Data Access Paradox

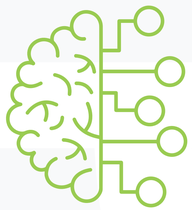
ROUNDMAP®

- Role-Based Access
- Secure Data Sharing
- Data Anonymization
- Secure Collaboration
- Data Masking
- Secure File Transfer
- Data Usage Policies
- Multi-Factor Authentication
- End-to-End Encryption
- Information Rights Mgt

A balanced approach to data sharing and security would involve implementing robust data governance frameworks that define clear access levels and permissions based on roles and responsibilities, ensuring that employees have access to the data they need while safeguarding sensitive information. It would also include regular audits, employee training on data ethics and privacy, and the use of encryption and other security technologies to protect data in transit and at rest, fostering a culture of security awareness alongside the promotion of collaboration and innovation.

- Encryption
- Access Control
- Data Governance
- Authentication
- Cybersecurity
- Risk Management
- Data Privacy
- Intrusion Detection
- Compliance Audits
- Data Encryption Standard (DES)

SHARING DATA



COLLECTIVE INSIGHTS

Sharing data is essential for fostering collaboration, innovation, and informed decision-making within an organization. However, unrestricted access to data can jeopardize the firm by exposing sensitive information to potential security threats and leading to data misuse or privacy violations.

BALANCE

SECURING DATA

DATA SILOS

Securing data is crucial to protect sensitive information from breaches and maintain trust within and outside the organization. However, an overly strict data regime can stifle the flow of information, hindering collective insights and diminishing the capacity for swift, empowered action in response to emerging challenges.