Data security in 2020 will be difficult. The epidemic made millions of people work from home. Cyberattacks from state actors attacked commercial databases. Natural calamities impacted enterprises and supply lines regionally. We interviewed 57 technology leaders in the second half of 2020, including CIOs, CISOs, CDOs, and other public- and private-sector business leaders. Cyber resilience, the capacity to endure unplanned interruption, is no longer the sole duty of IT. Companies require a comprehensive strategy to cyber resilience as data permeates operations and activities to improve business performance. They need a clear framework for managing all data and cross-functional responsibility for data security. Most companies were unprepared for the epidemic and the move to remote labour. Business and function executives might establish ad hoc arrangements for their staff. IT and security teams often didn't know which devices employees were using, the programmes on those devices, whether they had proper security patches, or the popularity of additional connected devices, such as game consoles and smart home gadgets. The consequent free-for-all for company activities increased cyber risk exponentially. Cyberattacks climbed 400% in 2020 compared to previous years due to bad actors abusing ill-secured virtual work environments and IT systems. 1 These assaults cost firms hundreds of thousands of dollars, but frequently much more, and cause many small and medium-sized businesses to fail. 2 Even though U.S. firm hack damages are expected to reach $1 trillion by 2020, just 44 organisations have cyber readiness and incident response strategies. Only 32 believed the strategy was effective, and the board or C-suite usually wasn't involved. SolarWinds' onslaught on government and Fortune 500 firms was scarier. Nearly 18,000 companies using SolarWinds IT management and network monitoring software had sensitive data exposed for eight months. 4 Worse, the attack inspired other crooks. Supply chain harm may not be known for months or years. It's over. Data is a competitive advantage for organisations in many industries, and digitalization will accelerate. Disruptions and threats put company data at danger. Given this complexity, firms require a data-driven, organization-wide strategy to cyber resilience. Data management accesses, stores, organises, and maintains an organization's data. Data must be accessible, comprehensible, connected, trustworthy, and secure. 5 Data must be safe in transit across a computer network or IT environment since network interfaces are typically vulnerable to outsiders. Data management questions need answers. Where does the organization's data live (databases, data warehouses, data lakes)? How often does data change and where does it go? Who has access to data, such as IT personnel, IoT devices, or other networks? Data use Is it converted or fed raw to corporate systems? How can data be accessed or locked in a natural disaster? How is the data examined for a cyberattack? How does the company track polluted data in IT? In answering all of these challenges, firms must find the correct balance between making data available and guaranteeing its security. They must also comprehend possible dangers and plan for their detection, reaction, and recovery. The entire organisation must be involved in planning and executing this project. IT and security professionals need actionable data on everything in the network, not just the devices and apps employees use. This involves advance planning to simulate data access scenarios and all conceivable network contact points, such as supply chain nodes. This requires cross-functional situational awareness across critical jobs. D.O. The CDO makes executive-level data management choices during regular operations and a breach. The CDO must classify and categorise data for business-critical activities and systems. Data categorizations come from data stewards in each business unit and function, who know their data needs. They know which personnel need access to certain data, which systems or feeds should have access, and how operational performance would be affected if some data were unavailable or tainted. Data stewards check data accuracy, promote exchanges, and map data flow. The IT staff includes cybersecurity engineers and enterprise architects. They determine how data enters and exits business systems and access security processes. The IT team instructs the workers on data management, including work-from-home restrictions, device limits, and company-owned hardware guidelines. HR. HR handles security clearances, work schedules, work-from-home rules, and employee requirements like VPNs. This information helps cyber resilience teams to immediately discover abnormalities in worker access to sensitive data and prioritise access after an attack. The legal department, including acquisitions and partnerships employees, collaborates with the CDO to ensure suppliers have crisis response agreements.