How to Assess the Resilience of Your System’s Data

The data dilemma

The stark reality is that without software, business halts—and without data, software is rendered impotent. The exponential growth of data is revolutionizing how we compete and operate. With enterprise software expenditures soaring to nearly $600 billion, up from $269 billion in 2011, the message is clear: harnessing data is not optional but essential for survival and prosperity. This intricate interdependence signals a looming crisis when either piece is compromised—a premise that leads us to the stark ramifications of data inaccessibility.

The consequences of inaccessible information

The consequences of inaccessible or mismanaged data can be devastating across various sectors. For instance, NASA’s $125 million Mars Orbiter was lost due to a simple data unit inconsistency. PayPal incurred government fines due to inadequate transaction screening. Sony’s PlayStation Network suffered a $2 billion loss from a security breach. And Toyota experienced a significant crisis that ground their manufacturing to a halt for two days.

Alarmingly, 93% of companies that lost their data center for 10 days or more due to a disaster, filed for bankruptcy within one year of the disaster. 50% of businesses that found themselves without data management for this same time period filed for bankruptcy immediately.

The need for data resiliency

These cases starkly demonstrate the dire consequences of failing to maintain robust, accessible data systems. By fostering data resilience, organizations can provide uninterrupted services despite external threats. This proactive approach not only safeguards against data loss and system downtimes but also ensures operational stability and continuity in the face of unforeseen challenges.

Additionally, organizations that embrace good data management practices lay a strong foundation for successful AI initiatives, as these programs are critically dependent on high-quality, well-organized data for optimal performance and accurate outcomes.

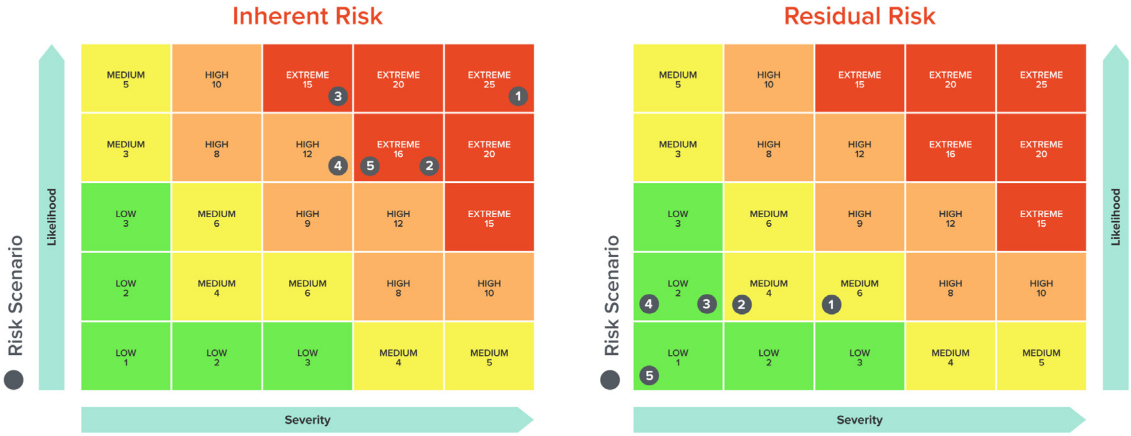
Table 1 shows the cause and potential impact of five common system and data availability risk scenarios. It also shows reflects the corresponding Inherent Risk scores for organizations that are yet to implement controls or mitigation strategies, followed by the potential Residual Risk scores after the deployment of Quest’s Data Resilience offering.

**Complex systems will fail.
Resilience is the ability to provide a service, despite the threat.**

- Ransomware attacks lead to an average of 16.2 days of downtime, with the average ransom payment in Q4 2021 spiking to $322,168
- The Toyota outage shows not all backup failures are ransomware
- A configuration error at CenturyLink led to 22 million customers in 39 states losing emergency 911 services for two days
- Global regulations now cover digital and operational resilience, reaching beyond finance to protect essential service providers across all sectors from disruptions
- 73% of surveyed professionals believe failing to invest in resilience will result in customer loss and a failure to innovate due to productivity losses

				Inherent Risk			Residual Risk		
Risk Scenario	Cause	Risk Event	Impact	Likelihood	Severity	Score	Likelihood	Severity	Score
1	Ransomware Attack	Stops all services, including internal operations and sales	Fines, reputations, revenue, and productivity impacts	5	5	25	3	2	6
2	Suboptimal Data Management and Governance	Non- compliance, increased vulnerability, poor governance	Poor decisions, waste, legal risk, harmed reputation, eroded trust	4	4	16	2	2	4
3	Outages of mission-critical application	Halts systems and services	Reduced revenue, customer satisfaction, reputation, morale and financial stability	3	5	15	2	1	2
4	Poor management of legacy technologies	System failures, breaches, and data loss	Reduced efficiency, increased costs and risks	3	4	12	2	1	2
5	Globally distributed data and data sovereignty	Breach of laws from improper global data storage	Fines, costly data shifts, reputation harm, trust loss, operational issues, and business downturn	4	4	16	1	2	2

Table 1. The cause and potential impact of five common system and data availability risk scenarios


Inherent Risk

Residual Risk

Table 2. The Inherent and Residual Risk scores of these five system and data risk scenarios are represented here on a 5x5 risk matrix.

How resilient is your system?

In today's digital world, data and system resilience are paramount. Quest offers guidance and solutions to enhance data and system availability, helping organizations architect for data resilience and navigate data threats. Our experts provide precise guidance, allowing your board of directors to incorporate data resilience into your business risk strategy.

We prioritize identifying crucial assets, safeguarding them, automating processes,ensuring data backups, enforcing immutability, optimizing offsite storage, and managing endpoints.

With Quest's support, you can bolster resilience and increase the value of your most crucial asset: data.

Quest Data & System Resilience Solution

- Speeds up the recovery from cyber threats
- Increases the intrinsic value of data
- Reduces risk of downtime
- Implements good data governance

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.