Rocket® software

Your Guide to Upgrading Your Mainframe's Infrastructure Resilience

Important management strategies for navigating IT's growing risks and complexity

Contents

03 Introduction

04 The consequences are heavy and fast

04 Understand your infrastructure resilience

05 Key infrastructure resilience components

06 Storage infrastructure is your cornerstone

06 You need your disaster recovery programs

07 Key disaster recovery program components

08 Data security and its significance in hybrid IT environments

09 How to build your resilient infrastructure

11 Conclusion

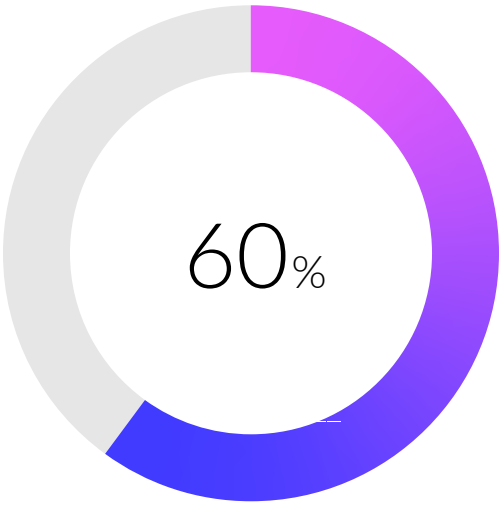
Introduction

For IT leaders and risk management professionals, prioritizing the right technology, processes, and education is crucial for developing a resilient infrastructure. According to Forrester, a resilient infrastructure is vital considering the 41% of surveyed IT leaders who named security and compliance as their top concern for modernization initiatives. And secure data handling was the leading objective among those initiatives, especially as IT environments grow increasingly complex, where system downtimes or data breaches lead to catastrophic consequences. Infrastructure resilience — especially with the mainframe — lives at the core of defense against cyberthreats as well as ensuring the health and integrity of operations amongst the evolving landscape of hybrid IT. This whitepaper will explore key strategies for enhancing infrastructure resilience, with a particular focus on mainframes.

← Back to contents

The consequences are heavy and fast

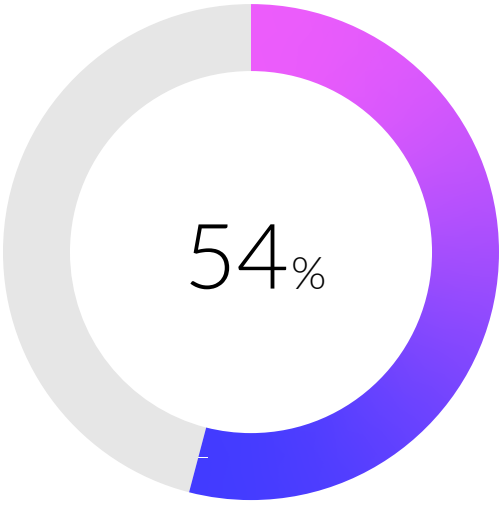
The cost of IT downtime now reaches up to $5 million[1] per hour in high-risk sectors, and non-compliance events cost an average of $4.88 million[2] in revenue loss. According to Gartner, organizations regularly find themselves with dated or inadequate disaster recovery (DR) plans in place, making them likely to lead to recovery failure or extended recovery operations.[3] And 60% of small businesses[4] close within six months of experiencing a significant cyber-attack. Yet only 54% of organization[5] have a company-wide disaster recovery plan in place. Failure to maintain operational integrity affects revenue, consumes extensive labor hours for resolution, and risks disruptive outcomes to reputation and brand that can be too devastating for recovery.



of small businesses close within six months of experiencing a significant cyber-attack.

Understand your infrastructure resilience

Infrastructure resilience refers to the proficiency of IT systems to withstand, adapt to, and recover from disruptions while ensuring minimal impact on operations. A resilient IT infrastructure incorporates several core components, each playing a pivotal role in fortifying systems to keep operations online and protect the trust and reliability built between a business and its clients.



Only 54% of organizations have a company-wide disaster recovery plan in place.

← Back to contents

Key infrastructure resilience components

01

Data encryption

The transformation of data into secure codes, rendering data unreadable to unauthorized users. This component is essential to creating a robust defense against cyber theft, protecting data during transit and at rest.

02

Data integrity

Assurance that the information remains accurate, consistent, and reliable over its lifecycle. Techniques like checksums and digital signatures are employed to detect and prevent data corruption, ensuring that the information remains trustworthy.

03

Vulnerability management

Proactive identification and mitigation of potential security weaknesses, such as regular vulnerability assessments and timely patch management which reduce the risk of exploitation.

04

Recovery and response

Efficacy in restoring operations and data after an incident, often including a well-structured disaster recovery plan along with regular backup procedures which ensure the quick return to normal function and the minimization of downtime and financial losses.

05

Authentication

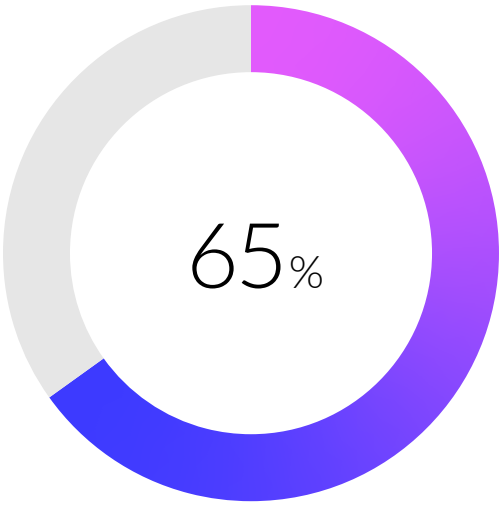
A network of secure access controls — fundamental for resilience, ensuring only authorized personnel can access sensitive systems and data. Implementing multi-factor authentication creates an additional layer of security, significantly decreasing the likelihood of unauthorized data access.

By incorporating these key components into an IT infrastructure, organizations function with confidence in their security and the safeguarding of both their operations and reputation.

← Back to contents

Storage infrastructure is your cornerstone

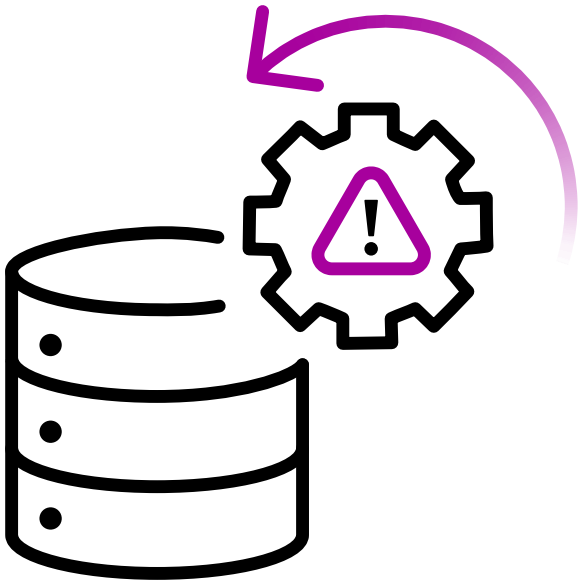
According to IDC[6] , data storage volume is growing by 65% compounded annually, with worldwide data expected to hit 175 zettabytes by 2025. z/OS generates 70% of operational data for banks, retailers, and large enterprises globally. While critical, this data growth also leads to exorbitant data storage costs, pressure to maintain a healthy data environment, strain on legacy storage solutions, and difficulty meeting compliance. Data has become the backbone of decision-making. Securing its accessibility — even amidst unforeseen circumstances — is essential for business continuity. Managing storage health proactively to prevent downtime, along with developing capabilities for rapid data recovery during outages, is critical.



Data storage volume is growing by 65% annually.

You need your disaster recovery programs

An effective disaster recovery program is non-negotiable. Comprehensive education, plans, and procedures must be in place to address potential outages. In light of the financial and reputational risks, the sophistication of your disaster recovery strategies fundamentally shape the future of your business.



← Back to contents

Key disaster recovery program components

01

Risk assessment

Identifying potential threats and vulnerabilities helps tailor the disaster recovery plan to address specific risks relevant to the business.

02

Comprehensive planning

Developing detailed recovery procedures for different scenarios ensures a structured response to various types of outages, from minor disruptions to major disasters.

03

Data backup and recovery

Backing up critical data and systems — with regularity — is vital for restoring operations quickly and accurately following an incident.

04

Communication strategies

Establishing clear communication channels keeps all stakeholders — including employees, customers, and partners — informed and coordinated during a crisis.

05

Regular testing and updates

Conducting routine drills and simulations helps identify strategic weaknesses and allows for timely updates to the business environment or technology.

06

Employee training

Educating staff about their roles and responsibilities in the event of a security incident empowers them to act swiftly and effectively when needed.

By integrating these components, businesses create resilient disaster recovery programs that mitigate the impact of disruptions and enhance overall organizational stability and trust.

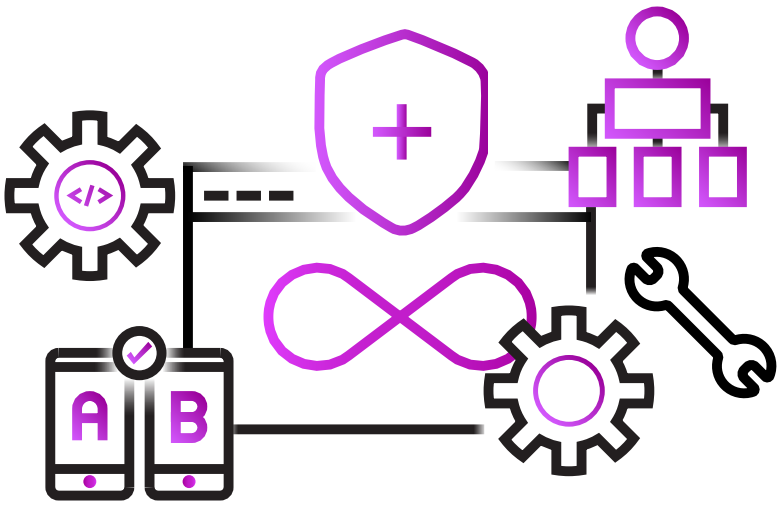
← Back to contents

Data security and its significance in hybrid IT environments

Hybrid IT environments make securing data more important than ever as organizations shift toward modernizing in place over re-platforming. This trend necessitates full access to data across various platforms, including on-premises systems, cloud environments, and other applications. Data sets travelling across these multiple touchpoints face increased risks, making appropriate security measures a vital need.

Securing data in hybrid environments involves encryption both in transit and at rest. Encryption in transit protects data as it moves between systems and applications, preventing interception by unauthorized parties. Encryption at rest safeguards data stored in databases and storage systems, providing a second layer of defense against potential breaches. Along with encryption, strong access controls and authentication mechanisms are also valued security tools.

Protecting your information and enhancing your operational efficiency and trust are dual benefits of prioritizing data security. Secure data access enables seamless collaboration and data sharing across applications, allowing organizations to leverage modern data replication and synchronization solutions confidently. A data security focus also ensures compliance with regulatory standards and fosters a secure environment for innovation and growth.



← Back to contents

How to build your resilient infrastructure

Let's get started

Create a strong disaster recovery program

Minimizing the costs and the operational impacts of an outage come from having the right disaster recovery plan for your business, founded on clear documentation and regular training to align all stakeholders with their roles and responsibilities.

To build a strong disaster recovery program, start by conducting a thorough risk assessment which identifies potential vulnerabilities. Develop a detailed recovery strategy that includes data backup and recovery procedures, communication plans, and resource allocation. Regularly test your recovery plan through simulations to ensure effectiveness and make necessary adjustments. Finally, continuously update your plan to accommodate new technologies and changing business needs.

Leverage technology that fits your infrastructure resilience

Advanced data recovery tools

Sophisticated data recovery tools supply essential precision and efficiency in restoring data. These tools are designed to recover specific data sets from precise points in time and minimize Recovery Point Objective (RPO) and Recovery Time Objective (RTO). By targeting exact data sets, businesses ensure a minimal loss of data and a swift return of operations — reducing downtime, cutting recovery costs, and enhancing the reliability of your infrastructure.

← Back to contents

Comprehensive data security

Investing in technologies that secure data across all platforms is essential for maintaining both integrity and accessibility throughout the data's lifecycle. The data remains unaltered and accessible to authorized users, preventing unauthorized changes or breaches. By securing data during transit —between the mainframe, the cloud, or other applications — organizations protect sensitive information. But keeping your data secure while at rest is equally critical, and both can be achieved through data encryption's ability to encode information.

Efficient ICF catalog maintenance

ICF (Integrated Catalog Facility) catalog maintenance technology supplies the proactive management of ICF catalogs, which prevents business disruptions and ensures seamless access to critical business data. This technology reduces the financial impact of catalog outages by reducing the threat of failure, speeding up recovery processes, and enhancing administrator productivity.

Educate and align your internal teams

Cultivate a culture where teams understand the importance of infrastructure resilience with regular training, testing, and clear documentation. The result? You'll have created readiness for disruptions and fostered swift, coordinated responses.

Continuous education on the role, responsibility, and process of team members during an outage is crucial for producing efficient and effective reactions. Comprehensive documentation serves as an additional guide for teams to rely on, minimizing confusion and enhancing the ability to manage disruptions smoothly.

Educating key stakeholders on the significance of infrastructure resilience is equally important. Communicating the company's prioritization of resilient infrastructure helps stakeholders understand the critical role they play. Their awareness and involvement are essential in both championing your mission and winning new investments for it.

← Back to contents

Conclusion

Infrastructure resilience is an ongoing commitment to security and operational excellence. Prioritize the right components, leverage enterprise storage, and adopt modernization trends. Do this in conjunction with employing advanced technologies and your organization will build a resilient infrastructure capable of withstanding modern challenges.

Ready to reinforce your organization's infrastructure resilience?

Speak with a Rocket Software expert and we'll assess your current resilience posture and develop a strategy tailored to your needs. Together, we'll ensure your business remains secure and competitive in an unpredictable world.

Speak to an expert

[1]Flower, D. (2024, April). The True Cost Of Downtime (And How To Avoid It). Forbes. https://www.forbes.com/councils/forbestechcouncil/2024/04/10/the-true-cost-of-downtime-and-how-to-avoid-it/

[2](2024). Cost of a Data Breach Report 2024. IBM. https://www.ibm.com/reports/data-breach

[3]Design and Document a Detailed Disaster Recovery Plan. Gartner. https://www.gartner.com/document-readerdocument/5639791?ref=solrAll&refval=437259537

[4](2024, October). Entrepreneurs Need to Stay Aware: Cybersecurity Threats May Indirectly Impact the Bottom Line. U.S. Small Business Administration. https://www.sba.gov/article/2024/10/03/entrepreneurs-need-stay-aware-cybersecurity-threats-may-directly-impact-bottom-line#:~:text=What%20today's%20small%20business%20owners,entrepreneur%20%248%2C000%20annually%20in%202023

[5](2021, June). Only 54% of organizations have a company-wide disaster recovery plan in place. Security Magazine. https://www.securitymagazine.com/articles/95521-only-54-of-organizations-have-a-company-wide-disaster-recovery-plan-in-place

[6](Siemasz, M). (2023, December). How Hybrid Cloud Solutions from Rocket Software Enables Businesses' IT Infrastructure to Remain Resilient. Rocket Software. https://www.rocketsoftware.com/blogs/how-hybrid-cloud-solutions-rocket-software-enables-businesses-it-infrastructure

About Rocket Software

Rocket Software is the global technology leader in modernization and partner of choice that empowers the world's leading businesses on their modernization journeys, spanning core systems to the cloud. Trusted by over 12,500 customers and 750 partners, and with more than 3,000 global employees, Rocket Software enables customers to maximize their data, applications, and infrastructure to deliver critical services that power our modern world. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located around the world. Rocket Software is a portfolio company of Bain Capital Private Equity. Follow Rocket Software on LinkedIn and X.

Rocket® software

Modernization. Without Disruption.™

Visit RocketSoftware.com ›

MAR-11850_Whitepaper_InfrastructureResilience_V3