primaryio Blog

EFFECTIVE CYBER RECOVERY REQUIRES PROPER DISASTER RECOVERY

By Mike Kail, CTO, PrimaryIO April 2024

A proper disaster recovery strategy is crucial for effective cyber recovery. Cyber recovery refers to the process of restoring systems, data, and operations after a cyber attack or security incident, such as a malware infection, data breach, or ransomware attack.

A comprehensive disaster recovery strategy is essential for cyber recovery for several reasons:

1. Data backup and restoration: A disaster recovery strategy typically includes regular data backups (or, ideally, continuous data replication) and procedures for restoring data from backups in the event of data loss or corruption due to a cyber attack. This ensures that critical data can be recovered and systems can be restored to a known good state.
2. System and application recovery: The strategy should outline the steps and procedures for recovering and rebuilding systems, applications, and infrastructure affected by a cyber attack. This may involve reinstalling software, restoring configurations, and rebuilding environments from backup images or clean sources.
3. Incident response and communication: A disaster recovery strategy should be closely integrated with an organization's incident response plan. It should define roles, responsibilities, and communication protocols for coordinating the recovery efforts and keeping stakeholders informed.
4. Testing and validation: Regular testing and validation of the disaster recovery strategy are crucial to ensure its effectiveness. This includes testing data restoration, system recovery, and failover procedures to identify and address any gaps or issues before an actual incident occurs.
5. Business continuity: Ultimately, the goal of a disaster recovery strategy is to minimize downtime and ensure business continuity in the event of a cyber attack or other disruptive event. It should outline procedures for maintaining critical operations, failover to alternate systems or locations, and prioritizing the recovery of mission-critical systems and data.

By having a well-designed and thoroughly tested disaster recovery strategy in place, organizations can significantly improve their cyber resilience, reduce the impact of cyber attacks, and minimize the time and effort required for recovery, ultimately protecting their operations, data, and reputation.

PrimaryIO provides a SaaS architecture Disaster Recovery as a Service platform subscription which includes continuous data replication from VMware VMs into an on-demand IBM Cloud VPC DR site. The product dashboard includes Firedrill test, a non-disruptive ability to assure that one can successfully recover in the event of a disaster. engage@primaryio.com