UBISTOR

White Paper

A COMPLETE DATA PROTECTION STRATEGY FOR CYBER RESILIENCE

The Unsung Heroes: Backup and Disaster Recovery-as-a-Service

Cybersecurity vs. Cyber Resilience

In today's digital era, cyber threats are growing at an alarming rate. A complete data protection strategy with robust security and recovery measures is more crucial than ever. This is where the concepts of cyber resilience, backup, and disaster recovery come into play. But first, let's distinguish between two commonly confused terms: cyber security and cyber resilience.

Cybersecurity focuses on protecting systems, networks, and data from cyber threats. It involves implementing measures to prevent unauthorized access, use, disclosure, disruption, or data destruction. The tools and strategies under cybersecurity are primarily geared towards prevention.

Cyber resilience is a broader concept. It encompasses cybersecurity's preventive measures and addresses how an organization responds to and recovers from cyber threats. It is about the ability to continue operating despite facing cyber threats and recovering quickly after an adverse event.

While cybersecurity is about prevention, cyber resilience is about bouncing back. Cyber security aims to prevent the storm; cyber resilience prepares you to weather it and emerge intact.

The Role of Backup and Disaster Recovery in Cyber Resilience

1. Backup-as-a-Service (BaaS): Backing up data is a cornerstone of a robust cyber resilience strategy. No system is foolproof, and there can be instances where data might be compromised, lost, or corrupted. Service providers such as UbiStor provide Backup as a Service, ensuring regular backups are consistently completing successfully, allowing an organization to restore its data to a point before the compromise, minimizing disruptions and data loss.

2. Disaster Recovery-as-a-Service (DRaaS): This cloud-based service allows businesses to recover their data and IT infrastructure during a disaster. DRaaS providers like UbiStor offer robust, geographically diverse solutions, ensuring that there are backups elsewhere if one data center faces issues. This means that operations can resume with minimal downtime, even in the face of major crises like natural disasters, ransomware attacks, or hardware failures.

Both backup and disaster recovery serve as safety nets, ensuring that the impact on business continuity is minimized even if a cyber-incident occurs. They are essential tools in the cyber resilience toolbox, allowing businesses to bounce back swiftly.

Why Backup is Essential in Cyber Resilience

1. Data Integrity and Availability: Backup solutions ensure that even if data is compromised, deleted, or encrypted (as in ransomware attacks), a copy is available to restore operations. This prevents data loss, which can be catastrophic for businesses.

2. Quick Recovery: Backups allow organizations to recover from cyber incidents swiftly, minimizing downtime. For businesses, time is money, and extended downtimes can have severe financial implications.

3. Historical Data Reference: Having backup versions from different points in time can be useful in case data becomes corrupted. It provides an avenue to return to an unaffected data version

Why Disaster Recovery is Essential in Cyber Resilience

1. Rapid Response: DRaaS solutions enable rapid recovery by providing a complete system replica in the cloud or another off-site location. This ensures business continuity even if the primary systems are compromised.
2. Cost-effective: Traditionally, disaster recovery required businesses to maintain duplicate sets of hardware and software. DRaaS reduces this cost by leveraging cloud resources only when needed.
3. Automated Testing: Many DRaaS solutions offer automated testing, ensuring recovery works when needed. This helps in instilling confidence in the organization's resilience strategy.
4. Geographical Redundancy: By leveraging cloud providers' vast infrastructure, DRaaS offers geographical redundancy, ensuring that local disasters (like power outages or natural disasters) don't halt operations.

Achieving Operational Integrity and Business Continuity

Cyber resilience, with its dual focus on prevention and recovery, ensures that businesses remain operational despite cyber threats. Backup and disaster recovery are central to this by guaranteeing data and operational integrity.

1. Reduced Downtime: Swift recovery translates to minimized downtime. For many online businesses, every minute of downtime can mean significant revenue loss.
2. Preserving Reputation: Customers and partners trust businesses with their data. Quick recovery from incidents preserves this trust and protects the organization's reputation.
3. Regulatory Compliance: Several industries have regulations regarding data protection and uptime. Backup-as-a-Service and DRaaS can ensure that businesses remain compliant, avoiding potential legal consequences and fines.
4. Financial Protection: Extended downtimes can result in substantial financial losses. By ensuring quick recovery, organizations protect their bottom line.

While cyber security is crucial for deterring threats, combining BaaS, DRaaS, and a broader cyber resilience strategy ensures business and operational continuity. In a world riddled with cyber threats, a comprehensive approach is needed to prepare businesses to prevent, respond, and recover – that is the key to long-term success.

About UbiStor:

Since 2001, UbiStor has been developing bulletproof data protection and disaster recovery strategies for their customers. With a consultative approach, UbiStor can cultivate strong relationships and perfectly constructed solutions for their customers, ensuring they are set up for success. Learn more at https://www.ubistor.com