CHECKLIST

Commvault®

Cyber Recovery Readiness Checklist

How to prepare, identify threats, assess the impact on business operations, and restore quickly.

01 **Identify all sensitive and critical data to address security and compliance concerns.**

Why is this important? Identify and classify your organization's data on a regular basis, including its age, ownership, and usefulness, so you can recover faster.

02 **Identify data anomalies and highlight potential data corruption or malware in a timely manner.**

Why is this important? Identify deviations from established behavioral baselines within your network to flag previously unknown types of ransomware and other cyber threats.

03 **Deploy decoys to intercept attacks before they reach their targets for early warning.**

Why is this important? Leverage cyber deception technology as a proactive defense that simultaneously alerts you to potential attacks in progress and slows down attacks by diverting bad actors toward fake assets.

04 **Implement "immutability" capabilities for critical backup data so that it is kept safe from any unauthorized changes.**

Why is this important? In the context of ransomware attacks, where attackers often attempt to encrypt or delete backups to force organizations into paying a ransom, this provides confidence that your backup data remains untouched.

05 **Deploy and test backup infrastructure to third-party hardening standards like CIS Level1.**

Why is this important? Infrastructure hardening minimizes the attack surface and strengthens the overall security posture of the system.

06 **Control who has access and level of access to your protected environment with specified layers of authorization.**

Why is this important? A security framework that rigorously validates and monitors user access, conducting continuous audits and implementing multiple layers of authorization, will help bolster security.

07 Protect and recover Active Directory as a whole or individual components.

Why is this important? AD is the key to your most critical assets – infrastructure and data – and a popular vector for ransomware attacks. Consider AD protection to keep your business running and cyber response strategies sound.

08 Store a tertiary copy of data in an isolated and air-gapped environment.

Why is this important? It effectively isolates and partitions secondary or tertiary backup copies from source environments, rendering them inaccessible from the corporate network. Coupled with immutable storage and the ability to quickly restore, it is an essential component to safeguard data against cyber threats.

09 Integrate backup and recovery solutions into existing SIEM and SOAR platforms to orchestrate and centralize events.

Why is this important? You can monitor, manage, and orchestrate actions and events from one central location, and quickly respond to any detected threats and protect backup assets with the appropriate actions.

10 Validate backup data is recoverable and no threats exist in copies before recovery.

Why is this important? It helps ensure that restored data is free from any contamination that could compromise the integrity and security of your organization's IT infrastructure.

11 Perform quarterly cyber recovery testing of all critical applications, and show demonstratable evidence of recovery readiness.

Why is this important? It helps verify that backup data can be successfully restored and data can be recovered to its original state in the event of a disaster, data loss, or system failure. It also provides the confidence that organizations can recover critical data and applications within acceptable timeframes and with minimal data loss.

12 Perform forensics securely in an isolated environment without causing any potential infections.

Why is this important? You can perform forensics like examine file metadata, timestamps, checksums, and other indicators of data integrity without causing further infections.

To learn more, visit **commvault.com**