CYBER RECOVERY VAULT

At a time when cyber-attacks are on the rise, it is imperative that you have a "critical data repository" - so that if the worse happens, you know that your critical data is isolated and available at a moment's notice.

"Did you know the average cyber-criminal only takes 17 minutes to access a network and remains dormant for 220 days before launching an attack?"

Why have a Cyber Recovery Solution?

- **Backup:** Bad actors can mount, delete, or encrypt backup data or catalogues, and often destroy the backup server.
- **Snaps:** Advanced cyber attackers can accumulate credentials and will often log in and delete snaps. They may destroy the entire platform, and there are "sleeperware" issues.
- **"Immutable" Snaps:** Despite the name, immutable copies can often be deleted or compromised, especially by insiders. So be careful of the definition. Snaps also tend to be platform specific.
- **Retention Lock:** This is a good hardening technique, but users still need to protect the catalogue. A failure or loss of the platform also compromises the whole structure.
- **Honey Pot:** End users setting up a sting operation for malicious activity by displaying data that appears to be a legitimate part of the infrastructure – but is isolated and monitored. Great, you have a small chance of finding the malicious activity – so if you get lucky, what do you do? How do you handle false positives?

The Cyber Recovery Vault creates a protected section of a data centre:

- The Cyber Recovery Vault is offline from the network (air-gapped and removed from the surface of attack). It is only accessible to users who have proper clearance.
- The solution includes management tools that "operationalise" a data recovery, starting with the creation and automation of recovery restore points.
- Restore points can be leveraged not just for recovery, but also for integrity checking and security-related analytics through the creation of sandbox copies.
- Analysis would take place on data-at-rest and cause no impact to the production environment. The sandbox copies could be the perfect way to perform offline malware/ransomware detection testing, such as looking for indicators of compromise or integrity attacks.
- Recovery is everything, this solution allows organisations to bring critical systems and data assets back online fast and securely.
- Organisations can leverage the expertise of our technical team, who offer proven methodologies for data protection, damage assessment, recovery, and remediation.

Don't be caught out, make sure you are protected today.

Speak to CSI to discuss your critical data insurance policy.

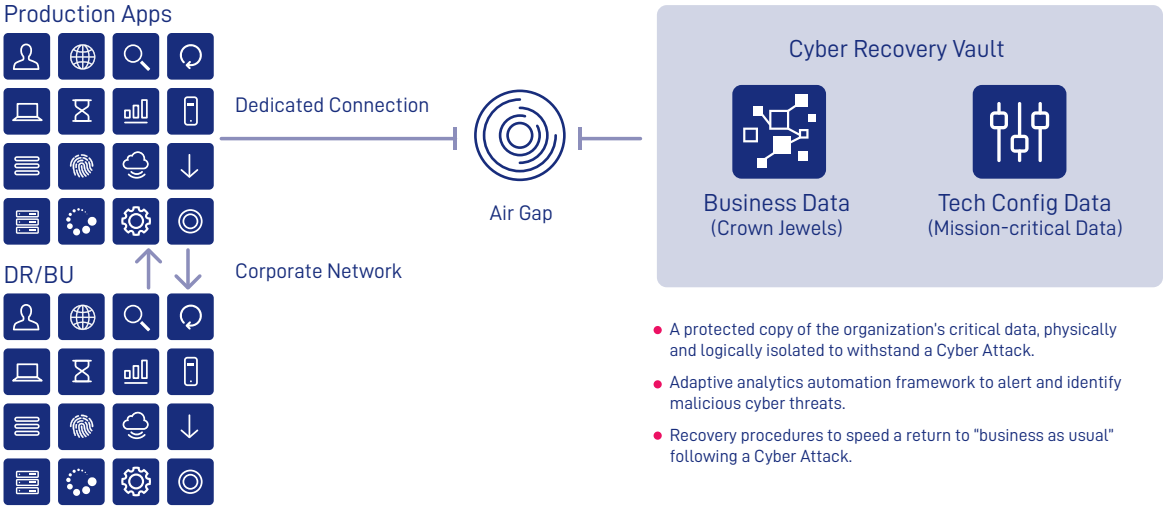
Cyber Recovery Strengths:

- Reduce overall potential attack surface
- Provide an isolated data vault environment that is disconnected from the network and restricted from users other than those with proper clearance
- Data transfer secured with a digital handshake, encryption of the replication link, and data payload
- Secure data copies through retention lock with governance or compliance mode
- Integrated analytics can provide a periodic analysis on the native backup set to find indicators of compromise
- Policy-based management and automation of the workflow
- Comprehensive reporting and modern user experience (UX) and HTML5 user interface (UI)

Benefits of Cyber Recovery Solutions:

- Protect data and enable recovery
- Security Analytics capabilities allow data in the Cyber Recovery Vault to be analysed in a secure environment, while the data is offline
- Optional solutions planning is available; we can deliver advanced consulting assistance to assist with the identification of business-critical systems/applications, current infrastructure, dependencies, recovery time and recovery point objectives, and other considerations
- Our consultative application dependency mapping service can help organisations understand their business environment, along with connections to other applications, common services, and outside suppliers. Understanding these dependencies can help identify risks
- Consulting services can integrate Cyber Recovery Solutions into response plans and include our methodology for damage assessments

THE SOLUTION: A RISK-BASED REPLICATION PROCESS



- A protected copy of the organization's critical data, physically and logically isolated to withstand a Cyber Attack.
- Adaptive analytics automation framework to alert and identify malicious cyber threats.
- Recovery procedures to speed a return to "business as usual" following a Cyber Attack.

Ransomware Protection:
Attackers cannot access the vault. There are no mount points accessible from production and no IP path into the vault.

Destructive Ransomware:
No access to vault target, and all data is retention locked. Even dormant malware cannot process or impact data that has been stored in the vault.

Insider or APT:
Cannot reach the vault without physical access; even then retention lock protects data from deletion.

Regulatory:
Provides a true "offline" or "operational Air gap" copy which is gaining traction in regulatory world.

Recovery Planning:
Provide clean room, run book development, focus on critical rebuild materials; advanced consulting can focus on dependencies and extreme RPOs and RTOs.

CSI UK Head Office
CSI House
2940 Trident Court
Birmingham Business Park
Solihull Parkway
Birmingham B37 7YN

CSI North America
379 West Broadway
New York
NY 10012

T +44 (0)800 1088 301
E INFO@YOURPERPETUALEDGE.COM
W YOURPERPETUALEDGE.COM