Backup Strategies:
Reconstituting Information is Key to Recovery

This paper outlines the best practices for #5 Backup Strategies.

Planning and Preparation Activities	***Recovery and Reconstitution Activities***
0. Disrupting the Attack Surface	
1. Architect to Protect *2. Secure Administration* *3. Access Control* *4. Device Hardening* ***5. Backup Strategies*** *6. Cyber Continuity of Operations (COOP) Planning*	*7. Cyber COOP Execution* *8. Secure Communications* *9. Core Services* *10. Data Recovery Strategies* *11. Forensics* *12. After Action Activities*

The BIG Idea

A properly structured backup infrastructure,for both information and systems, gives an organization the ability to recover from an otherwise catastrophic loss by restoring information and services.

Cyber Resiliency Goals & Objectives

Backups support the *Anticipate*[1] and *Recover* goals and *Understand*, *Prepare*, *Continue*, and *Reconstitute* objectives.

Design Principles

The design principles for Backups will help organizations prepare protected backups and improve the organization's ability to reconstitute information and services allowing the organization to continue with its mission.

- *Segmentation*: Ensure the backup data is isolated from other enterprise services to protect the backups from being impacted by adversary attacks.
- *Redundancy*: Deploy redundant systems in the Security Operations Center to provide failover capability; maintain protected copies of critical resources; design for spare capacity and secure failover.
- *Substantiated Integrity*: Ensure that adversaries have not corrupted backups of critical systems (e.g., directory servers, key management systems, payroll systems, etc); validate data provenance and integrity; validate software, service integrity, and system behavior to ensure they have not been corrupted.

What Can Be Done Now

The following resiliency techniques help organizations prepare protected Backups in order to recover information or systems that have been corrupted due to adversary tampering or system failure.

- *Segmentation*
  - Isolate backups from primary systems.
  - Logically and physically separate components based on degree of trust in system management and security.

[1] All italicized words are defined in the *Cyber Resiliency Terms and Concepts* document.

    - Replicate key functions and ensure segments are self-sufficient.
- *Redundancy*
    - Create and maintain protected copies of critical information.
    - Test failover systems to ensure proper operation.
- *Substantiated Integrity*
    - Test backup systems on a frequent basis and ensure the data is properly backed up.
    - Use an approved data integrity-verification technique (e.g., checksums) in conjunction with data backups as an indicator of data corruption.

The Right People & Policies

Creating a foundation of resiliency requires specific resources, skills, and policies, including:

- Budgets to provide life-cycle backup capabilities that are redundant, protected, and adequately segmented based on the needs of both IT and business operations.
- System Administrators and Storage Engineers to establish and maintain backups.
- Operating procedures for your security operations center that ensure regular backups and the processes to substantiate the integrity of the backups.

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques, *Redundancy* *Segmentation*, and *Substantiated Integrity*, as described above, defenders can impede the adversary's attack on the enterprise and limit the damage the malware causes. The use of *Segmentation* impedes the adversary's ability to employ mechanisms to manage the initial victims, execute the attack and hide their presense. The use of *Substantiated Integrity* enables the defenders to detect the malware if the adversary attempts to place it in the backups or use the backups to maintain their presense. The use of *Redundancy* in conjuncton with *Substantiated Integrity* enables the defenders to limit the adversary's ability to execute the attack.

Synergies & Barriers

Synergies among practices include S*egmentation* and *Substantiated Integrity*. *Segmentation* is made more effective when an organization also applies *Substantiated Integrity* capabilities to the enterprise.

Barriers to adoption include:

- Costs associated with maintaining and substantiating the integrity of segmented, protected, and redundant backups.
- Life-cycle costs, particularly for storage and systems.

Just Ahead

Backups are becoming a larger target for cyber adversaries. As defenders focus more on protecting the organization's infrastructure, they tend to forget about their backup services, making those the organization's soft underbelly. Attackers can corrupt the backup services to impede an organization's capability to restore systems and services. The

[2] The Cyber Attack Lifecycle is described in the *Cyber Attack Lifecycle and Resilience* document.

best approach is a combination of segmentation and privilege restriction to isolate, and advanced substantiated integrity to detect signs of backup corruption.

Creating portable or otherwise geographically disparate redundant assets and functionality will allow for a rapid recovery when standard backups or enclaves may be compromised by the adversary.