Data Recovery Strategies:
Assuring Trustworthiness for Continued Performance

This paper outlines the best practices for #10 Data Recovery 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

When an organization has experienced a cyber-attack, it must reconstitute its data and applications, including security infrastructure such as identity and access mechanisms, in order to continue mission or business critical functions in a trustworthy manner. This requires procedures for verifying the integrity of the backups to be restored, prioritization of restoration, and practices for ensuring that the destructive malware is not restored with the rest of the data.

Cyber Resiliency Goals & Objectives

The Data Recovery Strategies support the *Withstand*[1] and *Recover* goals and the *Continue* and *Reconstitute* objectives.

Design Principles

As the organization recovers from an incident the design principles for Data Recovery will ensure that critical data and applications are available, trustworthy, and restored in an appropriately prioritized order as determined by the Cyber COOP Planning. The following resiliency techniques provide support to these principles:

- *Adaptive Response:* Implement nimble cyber courses of action to manage risks.
- *Redundancy*: Provide multiple, diverse, protected instances of critical information and supporting services that will be used during the recovery process.
- *Substantiated Integrity*: Establish mechanisms to determine if critical infrastructure, services, information repositories, information streams and supporting components have been corrupted.

What Can Be Done Now

Adapt existing storage (e.g., backups and data centers) and verification mechanisms (e.g., anti- virus and monitoring technology) and define procedures to protect against adversary activities during the recovery process.

- *Adaptive Response*
    - Use configuration management and dynamic reconfiguration tools to incorporate replacement applications and data.

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

- *Redundancy*
  - Ensure that all tools and data involved in data recovery have backups.
  - Ensure that all individuals have adequately trained alternates, in the event the primary individuals are not available to implement data recovery procedures.
- *Substantiated Integrity*
  - Use the established system configuration baselines and the monitoring results to identify any adversary presence.
  - Verify the identity of an individual during the data recovery process before using information, direction or tools the individual has provided.

The Right People & Policies

Creating a foundation of resiliency requires specific skills and policies:

- Ensure project delivery and operational teams include traceable requirements for data resiliency and trustworthy operational components.
- Update disaster recovery policies and procedures that incorporate trustworthy operational components.
- Update testing policies, procedures and plans that include validation procedures for trustworthy data and service recovery.

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques, *Adaptive Response, Redundancy,* and *Substantiated Integrity*, as described above, defenders can impede and sometimes even preclude the adversary's efforts to maintain a presence in the enterprise and limit the damage the malware causes. The adversary's efforts to control initial victims, execute the attack plan and maintain a presence in the enterprise are limited by *Adaptive Response.* This technique reduces the time before data and applications are restored with clean copies. Using *Substantiated Integrity* with *Redundancy*, limits and impedes the adversary's abilities to:

- Control initial victims,
- Execute the attack plan and
- Maintain a presence in the enterprise.

Synergies & Barriers

Synergies among practices are based on *Adaptive Response's* use of both *Substantiated Integrity* and *Redundancy*. *Substantiated Integrity* provides capabilities such as behavior validation so that the redundant data and applications are validated before use.

Barriers to adoption include the following:

- Governance and standard operations, such as the potential conflict between the roles and responsibilities of system administration and systems recovery engineers.
- The cost of implementing and validating alternative/backup data and software.
- The cost of evolving and maintaining alternative courses of action, and training users on their use.
- Life-cycle cost of procuring, operating, and maintaining service recovery systems.

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

Just Ahead

Enterprise data recovery strategies should include *Redundancy* with *Diversity*, for example use different recovery mechanisms and software to mitigate the chance of malware attack. Enterprises should also, transition to the use of cryptographic checksums on data to help identify any efforts by malware to corrupt the data.