Core Services:

Re-establishing a Trusted Foundation

This paper outlines the best practices for #9 Core Services.

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

By properly rebuilding the high priority core services (*i.e.,* those key services needed for continuing an organization's critical missions and services) after an attack, an enterprise can ensure service integrity, expedite recovery, and minimize mission impact.

Cyber Resiliency Goals & Objectives

Core Services support the *Withstand*[1] and *Recover* goals and the *Continue*, *Constrain*, and *Reconstitute* objectives.

Design Principles

As the organization recovers from an incident, the design principles for Core Services will ensure that systems are restored via a process that balances trust and system dependencies with the requirements of the mission.

- *Adaptive Response*: Dynamically reconstitute critical assets or capabilities. Identify and restore functional capabilities based on criticality.
- *Coordinated Defense*: Coordinate recovery activities to avoid gaps in security coverage.
- *Redundancy*: Maintain multiple protected instances of hardware, software, and information, enabling a portion of service capacity to be quickly established.
- *Substantiated Integrity*: Validate data provenance. Validate data, software, and service integrity to ensure they are not corrupt.

What Can Be Done Now

Identify and prioritize all critical systems and their dependencies. Substantiate the integrity of the hardware, software and information stores, which will be used to restore these critical systems and their dependencies.

- *Adaptive Response*: Make sure the cyber playbooks include the list of critical systems and procedures for restoring each core service, including re-establishing security functionality in addition to mission critical systems.
- *Coordinated Defense*: Make sure the cyber playbooks identify dependencies between core services and provide guidance for ensuring services are restored in a manner and time, such that there are no gaps in those services.

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

- *Redundancy*: Make sure all critical systems have redundant backups of software, hardware, and data. Ensure current patch and configuration status of redundant firmware and software resources. Ensure protection of all instances of critical resources and backup systems regardless of location.
- *Substantiated Integrity*: Evaluate existing software integrity validation mechanisms and coverage. Identify ways to extend their coverage to include unprotected critical resources.

The Right People & Policies

- Policies and supporting processes for acquiring and maintaining redundant copies of hardware, software, and information.
- Policies and supporting processes for identifying the priority systems and their dependencies.

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques, *Coordinated Defense and Substantiated Integrity*, as described above, defenders can detect the adversary's attempts to control the initial victims of the attack and maintain a presence in the enterprise. These techniques together with *Adaptive Response* and *Redundancy* enable the defenders to impede the adversary's attempts to control the initial victims of the attack, execute the attack plan and maintain control. *Adaptive Response* together with *Redundancy* also enable defenders to limit the damage caused in these stages.

Synergies and Barriers

Synergies among practices include *Redundancy* and *Substantiated Integrity*. *Redundancy* reduces the likelihood of an attacker gaining control of all the targeted services, while *Redundancy* with *Substantiated Integrity* provides awareness of which systems are corrupted.

Barriers to adoption include the following:

- Governance and CONOPS issues, such as the potential conflict between the roles and responsibilities of system administration and service recovery engineers.
- The cost of implementing and validating data, software, and service integrity.
- Life-cycle cost of procuring, operating, and maintaining service recovery systems.
- Motivation for taking responsibility and ownership of the artifacts and procedures used for core services.

Just Ahead

In the future organization should consider introducing *diversity* into the set of techniques to support the core services. Organizations could maintain critical mission data across a diverse set of formats and backup solutions, possibly including the use of different types of hardware and software on components critical for recovery. The organization should also consider incorporating *Dynamic Positioning,* creating a version of core services that are located in a mobile unit (e.g., an RV) that would not be impacted by an attack on the main facilities. These techniques would increase the likelihood that some portion of the systems is in a position to recover in a timely manner from an adversary attack.

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