# Core Services

## Overview

Recovering from an incident, requires integrity in the core services (*i.e.,* those key services needed for continuing an organization's critical missions and services – these will differ from one organization to another) in order to keep cyber adversaries from inserting themselves into response and recovery processes. This document describes how to apply *Adaptive Response*[1], *Coordinated Defense, Redundancy,* and *Substantiated Integrity* resiliency techniques to assure integrity in the core services.

## Applying *Adaptive Response* to Limit Adversary Impacts

*Adaptive Response* – Implementing nimble cyber-courses-of-action to manage risks – Optimizes an organization's ability to respond in a timely and appropriate manner to adversary activities, thus maximizing the ability to maintain the integrity and availability of core services. There are three approaches to applying *adaptive response:*

- Dynamic Reconfiguration: Make changes to an element or component while it continues operating.
- Dynamic Resource Allocation: Change the allocation of resources to tasks or functions without terminating functions or processes.
- Adaptive Management: Change how defensive mechanisms are used based on changes in the operational environment as well as changes in the threat environment.

### Priorities for Immediate Action with *Adaptive Response*

The top priorities for *Adaptive Response* are:

- 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
- Ensure that adequate resources are allocated for alternate configurations that may be used when restoring core services under adverse conditions.

## Applying *Coordinated Defense* to Share Situational Awareness and Collaborate

*Coordinated Defense* – managing multiple, distinct mechanisms adaptively and in a coordinated way – can defend critical resources, such as core services, against adversary activities. There are two major implementation approaches to coordinated defense:

- Technical Defense-in-Depth: Make use of multiple protective mechanisms, applied at different architectural layers or locations (e.g., application, endpoints, network, and incident response perimeters).
- Coordination and Consistency Analysis: Apply processes, supported by analytic tools, to ensure that defenses are applied and cyber-courses–of-action are defined and executed in a coordinated, consistent, and non-disruptive way.

### Priorities for Immediate Action with *Coordinated Defense*

The top priorities for *Coordinated Defense* are:

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

- 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.
    - Ensure the cyber playbooks include re-establishing security functionality in addition to mission critical systems.
    - Coordinate among users, administrators, and managers of component systems.
    - Ensure that defenses are defined and implemented consistently across component systems and networks.
    - Test or simulate restoration processes to identify and eliminate any conflicts over critical resources.

## Applying *Redundancy* to Impede Adversary Actions

*Redundancy* – providing multiple protected instances of critical resources – can curtail the time during which the adversary can impact mission functions and degrade the extent of that impact.  There are three major implementation approaches to *redundancy*.

- Protected Backup and Restore: Back up information and software (including configuration data) in a way that protects its confidentiality, integrity, and authenticity, and to restore it in case of disruption or destruction.
- Surplus Capacity: Maintain enough extra capacity for information storage, processing, and/or communications to allow for restoration as systems and information grow.
- Replication: Duplicate information and/or functionality in multiple locations and keep it synchronized.

### Priorities for Immediate Action with *Redundancy*

- Make sure all critical systems have redundant backups of software, hardware, and data.
    - These should be safeguarded so they are not subject to the same adverse conditions as the primary core services but at the same time should be available to replace the primary core services within the time frame required.
    - Identify dependencies for the critical systems and ensure redundancy for these as well.
- Ensure current patch and configuration status of redundant firmware and software resources.
    - When primary firmware or software patches or configurations are updated and validated, update the redundant firmware and software.
- Ensure protection of all instances of critical resources and backup systems regardless of location.
    - The level of protection of critical resources should be the same whether they are the primary or the backup/secondary resource.
    - If different types of protection mechanisms are employed, assess these mechanisms to ensure they meet the minimum required protection level.

## Applying *Substantiated Integrity* to Curtail Exposure to the Adversary

*Substantiated Integrity* – ascertaining whether critical services, information stores, information streams, and components have been corrupted – can prevent an adversary from delivering a payload, curtail the adversary's impact and enable an enterprise to recover from an attack more effectively.  There are three approaches to *substantiated integrity*:

- Integrity/Quality Checks: Apply and validate checks of the integrity or quality of information, components, or services.
- Provenance Tracking: Identify and track the provenance of data, software, and/or hardware elements.

- Behavior Validation: Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage).

### Priorities for Immediate Action with *Substantiated Integrity*

- Evaluate existing software integrity and network address validation mechanisms and coverage. Identify ways to extend their coverage to include unprotected critical resources.
  - Use an approved data integrity-verification technique (e.g., checksums) as an indicator of data corruption.
  - Use tamper-evident technologies, checksums and other tools (e.g., code-canary like activities) to ensure the adversary has not tampered with core systems.

## Preparing for the Future

As new technology is incorporated into what is considered core services, practices must adjust. For example, appropriately incorporating virtualization into the policies and processes for maintaining redundancy offers both opportunity and challenges. Virtualization can vastly decrease the costs of redundancy but availability and separation concerns must be taken into consideration. In addition some challenges such as identifying priority systems and their dependencies will never disappear and may increase as new technologies change assumptions about connectivity and persistence.

Changes in technology almost always require changes in governance and concept of operations. These changes will bring conflicts between the roles and responsibilities of both system administrators and service recovery engineers. It is important to focus on the goals and resolve these conflicts in a way that does not leave gaps for the adversary to exploit.

The ability to withstand and recover from an incident relies heavily on the support of core services. Ensuring their presence is vital. Leveraging the synergies among resiliency techniques is critical to ensuring core services are available when needed. Incorporating elements of *Diversity* into *Redundancy* creates a more difficult environment for an attacker. An attack designed to target a homogenous environment will not be as effective in a heterogeneous environment. Likewise, incorporating *Substantiated Integrity* into *Redundancy* will provide early warning of compromised systems. This will enable defenders to limit or even prevent the corrupted systems from being used.

Resiliency can also be increased by incorporating D*ynamic Positioning* into *Redundancy*. For example providing an additional copy (or copies) of core services, situated outside the organizations usual perimeter in a mobile environment (e.g., an RV) increases resiliency by providing resources needed to recover from an attack that are unlikely to have been impacted by that attack.