Cyber Resiliency: Key Concepts & Terms

Cyber resiliency is the extent to which a nation, organization, or mission is able to withstand and rapidly recover from deliberate attacks, accidents, or naturally occurring threats to its critical cyber resources. Cyber resiliency is quickly emerging as a key component in any effective defense strategy. While cyber security is focused on keeping adversaries out, cyber resiliency is based on the assumption that an advanced adversary is not easily thwarted. Should the ongoing stresses of a persistent threat result in a successful attack, organizations must ensure that their essential functions can continue despite these adverse conditions.

Cyber security is designed to ensure that the objectives of confidentiality, integrity, availability, and accountability are achieved at acceptable levels. Cyber resiliency assumes that good cyber security practices are already in place—and then builds on them. Because cyber security functions, such as user identification and authentication, are prerequisites to other functionality, cyber resiliency techniques are particularly important to the architecture, design, and implementation of these functions.

Cyber Resiliency Activities

To be more resilient, organizations should engage in six key activities to prepare and plan for the inevitability of a cyber incursion (Pre-Bang) and six key activities to recover from an incursion once it has been detected (Post-Bang).

Pre-Bang

- **Architect to Protect:** Build resiliency into the foundation of your computing and communications infrastructure.
- **Secure Administration**: Incorporate resiliency into system administration and management to reduce the ability of the adversary to gain privileges and network access.
- **Access Control:** Constrain the adversary's courses of action to limit harm and increase resiliency.
- **Device Hardening:** Improve the defenses of component systems and services to make the attacker's job harder.
- **Backup Strategies:** Establish a foundation for recovering from an otherwise catastrophic loss.
- **Cyber Continuity of Operations (COOP) Planning**: Create a COOP plan that covers readiness (including the other five Pre-Bang activities), fighting through the attack, and recovering to an acceptable level of service—then practice it.

Post-Bang

- **Cyber COOP Execution:** Following the discovery of a cyber attack, execute your Cyber COOP plan.
- **Secure Communications:** Create a secure response infrastructure to keep cyber adversaries from inserting themselves into response and recovery processes.
- **Core Services:** Rebuild high-priority core services after an attack to ensure recovery and minimize disruption to the mission.
- **Data Recovery Strategies:** Execute your Pre-Bang Backup Strategies.
- **Forensics:** Forensics provides the information needed to ensure that an incident has been completely contained.
- **After Action Activities**: Review the cause and details of an incident to help the organization evolve its security architecture and identify areas where resilience capabilities can be enhanced.

Cyber Resiliency Engineering Framework

The Cyber Resiliency Engineering Aid includes the updated Cyber Resiliency Engineering Framework that will help your organization determine its resiliency goals and objectives and identify implementation approaches for achieving them.

Goals

- **Anticipate:** Maintain a state of informed preparedness to forestall compromises of mission function
- **Withstand:** Continue essential mission functions despite adverse conditions
- **Recover:** Restore mission functions during and after adverse conditions
- **Evolve:** Change mission functions or supporting capabilities to minimize future adverse impacts

Objectives

- **Understand:** Maintain useful representations of mission dependencies and resource status updates
- **Prepare:** Maintain a set of realistic courses of action that address predicted or anticipated adversity
- **Prevent/Avoid:** Preclude successful execution of attack or the manifestation of adverse conditions
- **Continue:** Maximize the duration and viability of essential mission functions during adverse conditions
- **Constrain:** Limit damage from adverse conditions
- **Reconstitute:** Redeploy resources to provide as much mission functionality as possible after adverse conditions
- **Transform:** Alter organizational behavior in response to prior, current, or potential adverse conditions
- **Re-architect:** Modify architectures for improved resilience

Cyber Resiliency Techniques

Each of the six recommended Pre-Bang and six recommended Post-Bang resiliency activities leverages a combination of techniques to maximize resiliency.

- **Adaptive Response:** Respond dynamically to specific situations, using agile and alternative operational contingencies to maintain minimum operational capabilities, limit consequences, and avoid destabilization
- **Analytic Monitoring:** Continuously gather, fuse, and analyze threat intelligence data to identify vulnerabilities, find indications of potential adverse conditions, and identify potential or actual damage
- **Coordinated Defense:** Coordinate multiple, distinct mechanisms (defense-in-depth) to protect critical resources across subsystems, boundaries, layers, systems, and organizations
- **Deception:** Establish a scope of deception (internal systems, supply chain, DMZ, etc.); confuse, deceive, and mislead the adversary
- **Diversity:** Use heterogeneous technologies, data sources, processing locations, and communication paths to minimize common mode failures (including attacks exploiting common vulnerabilities)
- **Dynamic Positioning:** Distribute and dynamically relocate functionality and assets to ensure consistent protection – this approach is also called a Moving Target Defense (MTD)
- **Dynamic Representation:** Identity and then expand upon static representations of components, systems, services, and adversary actions to support mission situation awareness and response
- **Non-Persistence:** Retain information, services, and connectivity for a limited time, thereby reducing exposure to corruption, modification, or usurpation
- **Privilege Restriction:** Design to restrict privileges assigned to users and cyber entities, and to set privilege requirements on resources based on criticality
- **Realignment:** Analyze mission processes to identify non-essential resources for offloading to reduce the attack surface, the potential for unintended consequences, and the potential for cascading failures
- **Redundancy:** Provide multiple protected instances of critical information and resources to reduce the consequences of loss
- **Segmentation:** Define and separate (logically or physically) components on the basis of criticality and trustworthiness to limit the spread of damage

- **Substantiated Integrity:** Provide mechanisms to ascertain whether critical services, information stores, information streams, and components have been corrupted
- **Unpredictability:** Make frequent and random changes to ensure that the attack surface is unpredictable