Cyber COOP Planning: Operationalizing Resiliency

This paper outlines the best practices for #6 Cyber Continuity of Operations (COOP) Planning.

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

To be resilient against threats of destructive malware, traditional continuity of operations (COOP) must be extended and integrated with cyber resilience into cyber architectures, and defender techniques, tactics and procedures (TTPs).

Cyber Resiliency Goals & Objectives

Cyber COOP supports the cyber resiliency *Anticipate* goal with *Understand*, *Prepare* and *Prevent*[1] as objectives.

Design Principles

The design principles for cyber COOP planning improve the capability of cyber systems, components and services to continue essential operations by preparing and planning for adversity.

Cyber COOP plans must consider core services, assign roles and responsibilities, and use proven tactics and procedures along with trusted communications. In addition, the verification and validation of cyber COOP plans is essential to successful recovery. This includes documenting the baseline network flow of traffic (net-flows) so incident response is more effective and enhanced forensics techniques are employed. Applicable resiliency techniques include:

- *Dynamic Representation*: Construct and maintain current representations of the posture of mission or business processes in light of cyber events and cyber courses of action. Provide cyber situational awareness as a part of overall situational awareness.
- *Coordinated Defense*: Plan, manage and coordinate multiple procedures and tactics along with the roles/responsibilities and playbooks needed for post-bang recovery.
- *Realignment:* Align cyber resources with core aspects of mission and business functions.

What Can Be Done Now

The following resiliency activities can be instituted now to maximize the effectiveness of cyber COOP planning:

- *Dynamic Representation*
  - Construct and maintain a dependency model, mapping functions to capabilities, services and systems.

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

  - Perform an impact analysis to determine crown jewels/core services and systems.
  - Define processes for updating the assessment of threat susceptibility for core services and systems.
- *Coordinated Defense*
  - Develop a cyber 'Go Bag' with essential procedures and information that would be needed during an incident.
  - Develop, test and validate playbooks, roles, responsibilities and tools (e.g., via tabletop type exercises).
  - Define collaboration processes and acquire tools for cyber defenders and incident responders.
- *Realignment*
  - Identify mission and business function dependencies on cyber resources (both direct and indirect).
  - Identify and eliminate non-mission and business function dependencies on, or uses of, cyber resources.
  - Assess mission and business function risks due to dependency on shared resources.

The Right People & Policies

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

- An enterprise architect who understands the potential consequences of APT activities and destructive malware along with the underlying concepts of Cyber resiliency goals, objectives and techniques.
- An entity SME who understands the entity mission and business objectives and the core services, capabilities and systems needed to provide essential operations to the organization.
- System administrators and cyber defenders with a culture of collaboration and shared situation awareness.
- Governance structures that enable the development and validation of COOP procedures.
- Strategic planning to ensure COOP evolves as core capabilities and systems evolve with technology growth.
- Budgets and resources for continuously testing, evaluating and updating COOP procedures.

Cyber Attack Lifecycle

Using the cyber resiliency techniques, *Dynamic Representation*, *Coordinated Defense,* and *Realignment,* defenders can detect and expose the adversary, impede the adversary's attack on the enterprise and limit the damage the malware causes. In some cases the defenders may even be able to preclude the adversary's efforts from having an impact. The use of *Coordinated Defense* and *Realignment* can impede the adversary's ability to initiate the exploit, take control of the initial victims, and execute an attack plan. The use of *Dynamic Representation* enables the defenders to detect and expose the adversary's efforts after the initial exploitation.

Synergies and Barriers

The organization SME must ensure that the Cyber COOP evolves as the core services, capabilities and systems evolve and are updated with new technology and capabilities.

Synergies among practice areas include *Dynamic Representation* and *Realignment* and *Coordinated Defense* and *Realignment*. Applying these practices will ensure COOP practices are well informed, validated and employ updated defender TTPs and data. Specifically,

- *Dynamic Representation* ensures critical mission/business functions are mapped to capabilities and systems, well understood and documented.
- *Coordinated Defense*, defines and validates key tactics and processes.
- *Realignment* aligns cyber resources with core aspects of mission/business functions.

Barriers to adoption include:

- Cultural resistance and lack of technology in keeping mission/business functions, capabilities and system mappings regularly updated.
- Time and costs related to performing, budgeting and maintaining regular COOP validation exercises and maintaining the Cyber 'Go Bag.'

Just Ahead

Cyber COOP planning must evolve to accommodate emerging technologies, such as those that enable automated mappings for functions, capabilities, services and systems. As another aspect of that evolution, versatile Cyber COOP planning must employ technologies and techniques that are fused with traditional COOP planning to increase its flexibility so its implementation can address the versatility of adversarial events that evolve and transform to respond to an organization's COOP actions. These types of technologies will enable an essential aspect of COOP – the continuous updates and validation of defender TTPs and processes. Finally, the evolution of COOP to address adversarial events means that the determination of the likelihood of an event happening (which is one factor that drives the selection of COOP technologies and techniques) is no longer based solely on historical evidence, but that the capability, intent and targeting of the adversary must be considered as well.