Cyber COOP Execution:
Facing Destructive Malware

This paper outlines the best practices for #7 Cyber Continuity of Operations (COOP) Execution.

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 to include cyber defense and incident response strategies and tools.

Cyber Resiliency Goals & Objectives

Cyber COOP Execution supports the cyber resiliency goal *Recover*[1] with *Continue*, *Reconstitute* and *Prevent* as objectives.

Design Principles

The design principles for Cyber COOP Execution improve the ability of cyber systems, components and services to continue mission or business essential objectives by recovering and reconstituting in the *post-bang* phase. In addition, forensics data is collected. For more information on that aspect, please see the guide on Forensics. Applicable resiliency techniques include:

- *Adaptive Response:* Use playbook cyber courses of action (CCoA) based on attack characteristics to recover to minimum core functionality, monitor effectiveness, and update CCoA as needed.
- *Analytic Monitoring*: Gather, fuse, and analyze data on an ongoing basis and in a coordinated way to identify potential vulnerabilities, adversary activities, and damage.
- *Substantiated Integrity:* Provide mechanisms to ascertain the integrity of reconstituted data, services, and information streams.

What Can Be Done Now

The following resiliency techniques can be applied now to maximize the effectiveness of Cyber COOP Execution:

- *Adaptive Response*
  - Perform continuous evaluation and modification of scenario information (e.g., incident and warning, and threat sharing) to stay abreast with the evolution of adversary attack vectors.
  - Notify facilities used for recovery that the organization has implemented its Cyber COOP, and it should prepare to receive Cyber COOP response and recovery personnel.

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

  - Integrate Cyber COOP Execution with other cyber resiliency functional areas to increase the dynamic capability of Cyber COOP response, recovery, and reconstitution.
- *Analytic Monitoring*
  - Identify the extent of damage to systems, applications, data, and resources caused by an adversary's actions.
  - Modify and continuously update CCoA quick-reference response guides.
  - Perform a complete assessment of Cyber COOP hardware, software, and data resources, both those in use and those staged to replace damaged resources, to assess the degree of damage or corruption those resources sustained and its impact to Cyber COOP response and recovery activities.
  - Incorporate into Cyber COOP recovery practices that complements forensic preservation.
- *Substantiated Integrity*
  - Execute procedures to validate the operational integrity of critical core systems, applications, components, and data that are used in Cyber COOP response and/or deployment at the COOP facility.
  - Verify the identities of the cyber source as well as the human source, of all data, software, and hardware before using the resource.
  - Ensure actions are taken to prevent re-infection during Cyber COOP Execution.

The Right People & Policies

Creating a foundation of resiliency requires specific skills and policies:

- 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 situational awareness.
- Governance structures that enable the development and validation of Cyber COOP procedures.
- Strategic planning to ensure Cyber COOP evolves as core capabilities and systems evolve with technology growth.
- Budgets and resources for continuously testing, evaluation and updating Cyber COOP procedures.

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques, *Adaptive Response, Analytic Monitoring,* 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. By using *Analytic Monitoring,* the defender is able to detect and analyze the adversary's efforts to control initial victims, execute the attack plan, and maintain a presence in the enterprise. The *Adaptive Response* technique can then be used to reduce the time before data and applications are restored while the *Substantiated Integrity* technique ensures that the data and applications restored are clean copies.

Synergies & Barriers

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

The three resiliency techniques discussed in this guide rely and support each other.

- *Adaptive Response* depends on *Analytic Monitoring* to ensure the responses are appropriate and uses *Substantiated Integrity* to ensure the adversary is not taking advantage of the chaos the attack has created.

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

- *Analytic Monitoring* also relies on *Substantiated Integrity* to ensure the data it is using has not been corrupted by the adversary.

Barriers to adoption include:

- Cultural resistance to coordination among administrators, as well as among administrators and cyber defenders.
- Life-cycle costs, particularly for architectural and design Diversity.
- The recognition that Cyber COOP Execution against an active, thinking, evolving adversary, requires a different mindset than Cyber COOP Execution against non-adversarial events.

Just Ahead

The enterprise architecture should accommodate emerging technologies, such as those that enable dynamic segmentation and resource isolation, and those used in synthetic diversity. It should also be able to accommodate new segmentation capabilities related to the Internet of Things, e.g., placing HVAC or lighting control services on a separate segment than business functions.