Cyber COOP Execution

Overview

Executing Cyber COOP operations in the wake of an adversarial attack using destructive malware requires integrating cyber resiliency concepts into the implementation of traditional COOP Execution. This document describes how to incorporate the cyber resiliency concepts of *Adaptive Response*[1]*, Analytic Monitoring, and Substantiated Integrity,* for more resilient Cyber COOP response, recovery and reconstitution.

Applying *Adaptive Response* to Restrain Adversary Impacts

Adaptive Response – implementing cyber courses of actions (CCoA) to respond dynamically to specific situations, using agile and alternative operational contingencies to maintain minimum operational capabilities, limit consequences and avoid destabilization. CCoA involve instituting pre-determined actions to help minimize and manage risks during Cyber COOP Execution. *Adaptive Response* optimizes an organization's capability to respond in a timely and appropriate manner to changing adversary activities, thus maximizing its capability to maintain the integrity and availability of core services. There are three approaches to applying A*daptive Response*, and all three are relevant to Cyber COOP Execution. Those three approaches are:

- 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.
- Dynamic Composability: Replace software elements with equivalent functionality without disrupting service.

Priorities for Immediate Action with *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.
    - Calibrate sensors and analyze data based on an understanding of the current risk posture.
    - Conduct periodic tests and exercises of Cyber COOP CCoA.
    - Conduct ongoing analysis of adversary actions and threats and monitor the effectiveness of CCoA against those actions and threats.
    - Coordinate with groups/consortiums of peer organizations to share threat and attack information.
- Integrate Cyber COOP Execution with other cyber resiliency functional areas to increase the dynamic capability of Cyber COOP response, recovery and reconstitution.
    - Identify an executive-level role as the accountable role for ensuring the integration of Cyber COOP response, recovery and reconstitution across organizational components.
    - Integrate functional-area incident definitions into Cyber COOP vocabulary so that triggering Cyber COOP responses is more targeted and flexible.
    - Develop easily accessible quick-response guides for possible cyber scenarios (i.e., compromise of information integrity, damage to physical IT assets, denial-of-service attack).
    - Implement recovery Cyber COOP containment processes (i.e., isolating compromised areas of the network) to limit collateral contamination and enable forensic observation.

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

  - Ensure redundancy in Cyber COOP response, recovery, and reconstitution components (i.e., hardware, software, personnel) so Cyber COOP Execution will be completed and executed without a full disruption to services.
  - Execute service-level agreements and relationships with external breach-remediation providers who can provide uncorrupted databases and applications (e.g., gold copies hosted on a clean virtual system).
  - Execute a mobility plan, if necessary, to get Cyber COOP response and recovery personnel and gold copies of applications and data to the Cyber COOP recovery facility (e.g., a "go bag" or "jump bag" as described in http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901).

Applying *Analytic Monitoring* to Detect and Preserve Adversary Actions

Analytic Monitoring – continuously gathering and analyzing data on an ongoing basis and in a coordinated way to identify potential vulnerabilities, adversary activities and damage – is implemented through several approaches, Monitoring and Damage Assessment (MD&A), Sensor Fusion and Analysis (SF&A), and Malware and Forensic Analysis (M&FA). Two *Analytic Monitoring* approaches, MD&A and M&FA, correlate with the execution of Cyber COOP activities.

- Monitoring and Damage Assessment: Behavior and characteristics of elements are monitored and analyzed to look for indicators of adversary activity, detect and assess damage, and watch for adversary activities during recovery and evolution.
- Malware and Forensic Analysis: Malware and other artifacts left behind by adversary activities are analyzed to develop observables, indicators, and adversary tactics, techniques, and procedures (TTP).

Priorities for Immediate Action with *Analytic Monitoring*

- Identify the extent of damage to systems, applications, data and resources caused by an adversary's actions.
  - Facilitate the creation of an initial damage assessment report that will be used to help determine the scope of Cyber COOP response and recovery activities.
  - Coordinate Cyber COOP activities with other cyber security functional area activities to provide a consolidated and dynamic response and recovery capability against adversarial attacks.
  - Implement notification and activation procedures to alert and mobilize Cyber COOP recovery teams.
- Modify and continuously update Cyber COOP quick-reference response guides.
  - Ensure integrity of recovery operations by making sure all individuals responsible for data recovery have adequately trained alternates who are available to implement data recovery procedures in the event the primary individuals are not available.
- Perform a complete assessment of Cyber COOP hardware, software and data resources, both impacted and staged, to assess the degree of damage or corruption those resources sustained and its impact to Cyber COOP response and recovery activities.
  - Communicate and correlate the results of that assessment to the Cyber COOP operations center and/or other cyber response functional groups such as the Cyber Security Incident Response Team.
  - Monitor Cyber COOP hardware, software and data resources for any signs of corruption.
  - Monitor availability and readiness of Cyber COOP personnel resources to fulfill their Cyber COOP roles and responsibilities.
- Incorporate into Cyber COOP recovery practices that complements forensic preservation.
  - Protect integrity of forensic data during recovery.

Applying *Substantiated Integrity* to Impede Adversarial Propagation

Substantiated Integrity – ascertaining whether critical services, information stores, information streams, and components have been corrupted – can help ensure the effectiveness of overall Cyber COOP operations and reduce the time, scope and resources needed to execute effective recovery operations. There are three approaches to *Substantiated Integrity*:

- Integrity Checks: Apply and validate checks of the integrity 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*

- 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.
    - Employ tools and processes for checking integrity of data, services and information streams. (e.g., Use a validated Gold Copy of system and application software so recovery operations are based upon a clean foundation. If there are no checksums validating data integrity against other copies is another option.)
    - Perform isolated integrity checks on critical workstations, servers, mobile computing devices, firewalls, e-mail servers, and remote access servers.
    - Validate the data before and after recovery and reconstitution as well as the results received from processing the data. Identify mechanisms to compare the baselines with monitoring data.
- Verify the identities of the cyber source as well as the human source, of all data, software, and hardware before using the resource.
    - Establish and implement processes for identifying individuals using both in-band and out-of-band procedures that are not vulnerable to the same types of attack. Ensure only officially identified COOP personnel are performing recovery and reconstitution activities, especially at the COOP facility.
    - Establish and update the list of authorized individuals who will be providing information, direction and tools during a time when data recovery processes are implemented.
- Ensure actions are taken to prevent re-infection during COOP Execution. Some of those actions may be to:
    - Apply more vigilant and stringent execution of physical, electronic access and rules of behavior (ROB) control procedures to minimize the threat of an insider threat or insider accommodation.
    - Change email settings to prevent a file attachment type from being allowed through the restored email system.
    - Implement a phased enablement of critical services, and disable all unused services.
    - Utilize virtualization techniques like snapshotting systems at critical points of recovery to enable rollback capabilities in case of unknown infection vectors.

Preparing for the Future

The new frontier of complex interconnectedness of the Internet of Things (IoT) and the ever-evolving metastasizing of malware and other cyber threat actors are challenges to effective Cyber COOP Execution, but challenges that are an opportunity to make Cyber COOP TTPs stronger and more effective.

Cyber COOP must be melded with traditional COOP methodologies to forge a muscled, turnkey approach for not only executing successful and effective Cyber COOP operations, but also helping to preserve traceability for forensic operations. Cyber COOP must continue to explore and expand integrating technologies such as automated, on-the-fly

alert and notification software, and integrated planning software that promotes both the planning and the execution of Cyber COOP tasks. A taxonomy of risks, threats, threat indicators, potential failure modes, attack scenarios, and Cyber COOP heuristics should be developed and updated continually. Managed-service providers should be considered to provide virtualized recovery operations, isolation, and dependency mapping and recovery, especially for critical components and systems. Cyber COOP Execution must support the mission of sustaining the business operations, and must be focused on supporting them, whether the business involves the defense of a nation or keeping life support systems operational during a power outage. Cyber COOP personnel must receive updated training on their roles and responsibilities as the threat environment changes or new technology is introduced. And lastly, Cyber COOPs must be kept up-to-date and tested periodically.