

## **Introduction**

NIST is developing a technology-neutral guide to assist federal agencies and other organizations in improving their cyber event recovery plans, processes, and procedures, with the goal of resuming normal operations more quickly. The guide will extend, and will not replace, existing federal guidelines regarding incident response or industry best practices by providing actionable information specifically on preparing for cyber event recovery and achieving continuous improvement of recovery capabilities. It will reference existing guidance for recovery of information technology.

On April 7, 2016, NIST will conduct a workshop where participants will share their experiences and provide additional input for the recovery publication. In support of that workshop, NIST is providing this preliminary information as an overview of the current publication content. The content was gathered from existing resources, including standard best practices related to recovery, as well as input from other government agencies and data from industry collaborators. The main topics that will be covered in the recovery publication are recovery planning, continuous improvement, recovery metrics, and example scenarios.

## **Recovery Planning**

Recovery planning includes identification and creation of processes and procedures that will be used to ensure continued operation and/or restoration of mission-critical functions in the face of a cyber event.

### ***Improving Enterprise Resiliency***

The organization should improve its enterprise resiliency, which refers to the organization's ability to continue to provide, or restore provision of, mission-critical functions despite a cyber event. Considerations include:

- Understanding how to be resilient, i.e., planning how to operate in a diminished capacity or restore services over time based on relative priorities.
- Identifying and documenting the key personnel who will be responsible for defining recovery criteria and associated plans, and ensuring that these personnel understand their roles and responsibilities.
- Creating and maintaining a list of the people, process, and technology assets that enable the organization to achieve its mission, along with all dependencies among these assets.
- Documenting and maintaining categorizations for these assets based on their relative importance and interdependencies to enable prioritization of recovery efforts.

### ***Process and Procedure Development***

The organization should develop recovery processes and procedures to ensure timely restoration of systems and other assets affected by future cyber events. This should include:

- Development of comprehensive plans for recovery that support prioritization and recovery objectives.
- Use of these plans as the basis for developing recovery processes and procedures that ensure timely restoration of systems and other assets affected by future cyber events. The processes and procedures should address both technical and non-technical actions affecting people, processes, and technologies.
- Implementation of practice-specific recovery procedures based upon the above-referenced processes.

### ***Definition of Recovery Initiation, Intermediate Goals, and Termination***

The organization should formally define and document criteria for specific milestones in the cyber event recovery lifecycle, including when a recovery plan is invoked, when recovery is considered successful, and when the recovery process is finished.

Considerations include:

- Formal definition and documentation of the conditions under which the recovery plan is to be invoked, who has the authority to invoke the plan, and how recovery personnel will be notified of the need for recovery activities to be performed.
- Definition of key milestones for meeting intermediate recovery goals and terminating active recovery efforts.

### ***Root Cause Determination***

The organization should definitively understand the causes of a cyber event as an important element of successful recovery. Root cause determination should occur before recovery efforts start in earnest, in order to properly adjust incident detection and response policies, processes, and procedures.

### ***Recovery Communications Planning***

Recovery communications includes processes that ensure that restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, vendors). It also includes any public relations activities that might be required because of the event. Considerations for recovery communications planning include:

- Development of a comprehensive recovery communications plan that fully integrates communications considerations into recovery policies, plans, processes, and procedures.
- Consideration of whether and how the organization might share actionable information about cyber threats with other organizations. This aspect would include preparation of sharing criteria including definition of information sharing goals, objectives, scope, and rules.
- Establishment of guidelines regarding what information may and/or should be shared with each type of constituent.
- Implementation and maintenance of current points of contact for each type of stakeholder to minimize delays during the recovery process.

## **Continuous Improvement**

Continuous improvement is an organizational mindset that focuses on an ongoing effort to improve. Concerning cyber event recovery, this approach supports the continual application of capabilities, described below, that ensure the organization's resilience in light of attacks.

### ***Validating Recovery Capabilities***

The organization should test and validate all of its recovery capabilities in order to ensure they are able to restore mission-critical functions. Validation activities include:

- Use of a combination of exercises and tests to periodically confirm recovery capabilities. A realistic and comprehensive review of the results of the exercise or test is important to fully understand an organization's recovery capabilities.
- Solicitation of input from various individuals with recovery responsibilities to improve recovery exercises and tests.

### ***Improving Recovery and Security Capabilities***

The organization should define specific methods to learn from gaps that are identified during the recovery process, either as part of the recovery plan or the organization's security posture, and integrating improvements into future planning and recovery. Considerations include:

- Continually improving cyber event recovery plans, policies, and procedures by addressing lessons learned during recovery efforts and by periodically validating the recovery capabilities themselves.
- Recording identified issues during the recovery activities so that personnel may subsequently expand on their documentation, either later in the recovery process or immediately after recovery activities are complete.
- Using recovery as a mechanism for identifying weaknesses in the organization's technologies, processes, and personnel. The weaknesses identified can be used to inform the other functions of the cyber security framework to improve the organization's security posture and the ability to meet its mission.
- Measuring and analyzing current and past cyber event recovery efforts to identify resilience weaknesses. Analysis may help identify how available resources can best be applied to address discovered issues.

## **Recovery Metrics**

The use of recovery metrics serves multiple purposes, helping to measure the performance of the defined processes and illustrating ways to improve them. Metrics may support reporting needs (such as in response to an inquiry from an external authority) as well as information sharing. Pre-determining what will be measured, and with whom metrics will be shared, will aid in managing and monitoring the organization's recovery efforts.

## **Example Scenarios**

The guide will present example scenarios that illustrate how, using the recommendations described previously, organizations can effectively recover from cyber events and subsequently use information gained during events to improve cybersecurity processes. The scenarios are not meant to be all inclusive or exhaustive of cyber events, but to provide a means to demonstrate how to apply the guide's recommendations for a specific situation.

**Scenario 1** - This scenario will describe an organization that has experienced a significant breach of its information network. Anomalous activity was detected during recent log reviews, indicating that a malicious actor used stolen credentials to gain access to one or more critical information systems.

**Scenario 2** - This scenario will describe an organization that is the victim of a destructive instance of malicious software. The malicious actor has installed ransomware on internal financial systems and is demanding payment, stating that they will wipe out all the financial records if payment is not received. As a warning, the adversary launches a zero-day attack against an important payroll system, permanently destroying the firmware of that server and several workstations that access the system.