ITL BULLETIN FOR FEBRUARY 2017

GUIDE FOR CYBERSECURITY INCIDENT RECOVERY

Murugiah Souppaya, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

In light of the recent number of cybersecurity (cyber) incidents, it is critical that organizations be able to conduct rapid and effective incident recovery. In a perfect world, avoiding all such incidents would be the best scenario, but reality shows that some organizations will eventually need to recover from an incident. An effective organizational defense-in-depth strategy combines the ability to improve its prevention capabilities, such as with effective training and modern technology, while also augmenting cyber event detection and response capabilities to inform and improve protection.

In 2015, members of the federal government reviewed cybersecurity capabilities and, as documented in the *Cybersecurity Strategy and Implementation Plan (CSIP)*, identified the need for improved policies and plans for responding to and recovering from evolving and sophisticated threats. Although guidelines existed on cyber incident handling, none of them focused on improving cybersecurity recovery capabilities, and the fundamental information was not captured in a single document. Previous recovery content tended to be spread out across topics such as general security, contingency, disaster recovery, and business continuity plans. Recovery is an important element of the enterprise risk management process life cycle; for example, the *Framework for Improving Critical Infrastructure Cybersecurity (CSF)*[2] includes it among the five core functions critical for a complete defense: Identify, Protect, Detect, Respond, and Recover.

NIST recently published Special Publication (SP) 800-184, *Guide for Cybersecurity Event Recovery*, which focuses on two phases of recovery: tactical and strategic. The immediate tactical recovery phase is achieved largely through the execution of the recovery playbook, as planned prior to the incident (with input from Detect and other CSF functions as required). The second phase is more strategic and focuses on the continuous improvement of all of the CSF functions to mitigate the likelihood and impact of

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.
[2] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, February 12, 2014.
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

future cyber incidents (based on the lessons learned from the incident as well as from other organization and industry practices).

NIST SP 800-184 provides guidance to help organizations, in a technology-neutral way, to plan and prepare for recovery from a cyber incident and to integrate the processes and procedures into enterprise risk management plans. It is not intended for use while responding to an active cyber event, but as a guide to develop recovery plans, in the form of customized playbooks, before an incident occurs. While many fundamental activities are similar for organizations of different sizes and from different industry sectors, each playbook can focus on a unique type of cyber incident and can be organization-specific, tailored to fit the dependencies of its people, processes, and technologies.

Planning for Cyber Incident Recovery

The guidance document emphasizes that effective planning is a critical component of an organization's preparedness for cyber event recovery. As part of an ongoing organizational information security program, recovery planning enables participants to consider system dependencies; critical personnel identities such as crisis management and incident management roles; arrangements for alternate communication channels, services, and facilities; and many other elements of business continuity. Planning also enables the organization to explore "what if" scenarios, which might be based largely on recent cyber events that have negatively affected other organizations, to develop customized playbooks. Analyzing each scenario helps the organization to evaluate the potential impact, planned response activities, and resulting recovery processes long before an actual cyber event takes place. Exercises help to identify gaps that can be addressed before a crisis situation, reducing the impact of an incident. Such scenarios also help to exercise both technical and nontechnical aspects of recovery such as personnel considerations, legal concerns, and facility issues.

NIST SP 800-184 describes the importance of improving and integrating cyber event recovery planning with security operations. The primary purpose of the guidance is to help organizations gain better resilience through better-prepared plans and playbooks. While the details of the recovery plan need to be developed by each organization, the guidance document defines topics that a typical plan might include and provides the list of key recommendations on cyber event recovery planning.

Continuous Improvement

One of the aspects highlighted by the new document is that cyber event recovery planning is not a one-time activity. The plans, policies, and procedures created for recovery should be continually improved by addressing lessons learned during recovery efforts and by periodically validating the recovery capabilities themselves due to changes in technology and the threat landscape. Since the outcome of these types of identifications will help define long-term goals for the organization, continuous improvement of the recovery plan is part of the strategic phase. As well as giving insights into improving

an organization's recovery capabilities and security posture, the document provides a summary of recovery improvement activities; these include different ways of validating recovery capabilities and using recovery as a mechanism for identifying weaknesses in the organization's technologies, processes, and people that should be addressed to improve the organization's security posture and the ability to meet its mission.

Recovery Metrics

Throughout the process of planning, exercising, and executing recovery activities, the collection of specific metrics may help to improve recovery and inform continuous improvement. Determining these metrics in advance may be beneficial, both to understand what should be measured and to implement data collection processes. This process requires the ability to determine where those identified metrics can be most beneficial to the recovery activity and to identify which activities cannot be measured in an accurate and repeatable way. It is important to note that restoring business functions remains the primary task at hand; the collection of recovery metrics can be designed in a way such that data is a natural output of recovery activities. Metrics can be detrimental if they hinder the recovery process, cause a rushed/incomplete investigation, or create additional obstacles for recovery team efficiency. It is critical to ensure that metrics provide useful information that supports actionable improvement without being harmful to recovery.

NIST SP 800-184 states that the majority of recovery metrics will be used to improve the quality of the organization's recovery actions. Recovery metrics might, for example, help to improve specific recovery aspects or be used to perform a cost/benefit analysis of a particular approach. Other metrics might be used as part of compulsory reporting (such as in response to an inquiry from an external authority) or for information sharing. In each case, determining in advance what will be measured and which measures may be shared will aid the organization's recovery efforts. Sharing metrics with others must be done with caution and should occur only with the approval of appropriate organizational stakeholders, including senior managers, legal representatives, and regulatory compliance personnel.

Building the Playbook

The organization's information gathering and planning activities provide substantial understanding about mission-supporting information systems, including those systems' dependencies and intricacies. This foundational understanding is critical to enable business functions to operate even under normal conditions. During a cyber event, this information becomes even more paramount, so processes and procedures need to be presented in an actionable manner to effectively restore business functions quickly and holistically. The playbook is a way to express the required recovery tasks and processes in a manner that provides relevant actions and milestones for each organization's systems.

The *Building the Playbook* section of the document summarizes recommendations described in the previous sections to provide a consolidated list of items that can be included in a playbook. Recovery activities are organized in two phases:

1. The initial tactical recovery phase is achieved largely through execution of the playbook developed as part of the planning efforts for cyber event recovery. This playbook prepares the organization for the recovery actions themselves, building upon activities performed during the protection, detection, and response functions of the enterprise risk management life-cycle process. The actions can be organized into initiation, execution, and termination stages.

2. The second, more strategic, phase focuses on the continuous improvement of the organization risk management process life cycle, as driven by the recovery activities. This second phase looks at how to reduce the organization's attack surface and minimize cyber threats. Actions can be further organized into the planning/execution, metrics, and recovery improvement stages. Lessons learned in exercises and previous recoveries help to identify gaps and to inform the planning and execution of other CSF functions.

Examples of Recovery Scenarios

NIST SP 800-184 presents two example scenarios that illustrate how, using the guidelines provided in earlier sections of the document, organizations can effectively recover from a fictional but realistic data breach. The first scenario focuses on an exfiltration attack including possibilities of the loss of significant amounts of personally identifiable information (PII) and customer financial data. A second scenario focuses on the real-world issues of a ransomware attack affecting a significant percentage of end user systems, with the possibility that the ransomware could spread to other systems.

For both scenarios, the section walks the reader through pre-considerations required for an effective recovery; the steps involved in successfully initiating, executing, and terminating a tactical recovery phase; and considerations for the strategic recovery phase.

Both scenarios are fictional and not meant to be all-inclusive or exhaustive, but they provide a way to demonstrate how to apply the document's recommendations and how to use a recovery playbook. In particular, the examples demonstrate the need to use information gained during the recovery process to improve cybersecurity processes.

Conclusion

NIST SP 800-184 provides guidance to help organizations with integrating comprehensive recovery planning and realistic test scenarios into risk management processes. Preparation supports rapid and effective recovery from incidents, and helps to minimize the impact of an incident on the organization and its constituents. Additionally, continual improvement of recovery planning, such as through learning

from previous events, including those of other organizations, helps to ensure the continuity of important mission functions.

The document supports tactical and strategic guidance regarding planning, development, testing, and improvement of a recovery playbook. It illustrates the mapping among recovery processes/activities to CSF subcategories and to related NIST SP 800-53 Revision 4 security controls. The publication's example scenarios demonstrate how to apply the guidance and how informative metrics may be helpful for improving resilience of information systems.

Additional Resource

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov