NIST SP 800-184: Guide for Cybersecurity Event Recovery
• Purpose
  • Provide guidance to prepare for recovery from a cyber incident
  • Previous recovery content tended to be spread out
  • Important to enterprise risk management

• Our Approach
  • Open & Transparent
  • Impartial facilitator and convener
  • Collaborate with USG and Industry
  • Include current industry and government standards and practices
NIST Cybersecurity Framework (CSF)

- NIST published the Cybersecurity Framework to help organizations manage cybersecurity risks.

- Recover is one of the five core functions of the CSF.

- Recovery is the development and implementation of plans, processes, and procedures for recovery and full restoration, in a timely manner, of any capabilities or services that are impaired due to a cyber event.
NIST SP 800-184 Relation to CSF
NIST SP 800-184 Guidance

- Planning for Cyber Event Recovery
- Continuous Improvement
- Recovery Metrics
- Building the Playbook
- Example Scenarios of Cyber Events
Planning for Cyber Event Recovery

• Understand people, processes, and technologies and their interdependencies.
• Define key milestones for recovery efforts.
• Implement effective incident management policies.
• Develop a comprehensive recovery communications plan.
Continuous Improvement

• Implement cyber event recovery exercises and tests.
• Conduct post exercise debriefs to incorporate lessons learned.
• Use recovery to enhance organization’s security posture.
• Record issues to expand on existing system documentation.
Recovery Metrics

- Organizations define what metrics to use and how to use them.
- Ensure metrics provide useful information that supports actionable improvement without being detrimental to recovery.
- Example Metrics:
  - Legal costs [dollar]
  - Hardware, software, and labor costs [dollar]
  - Costs relating to business disruption (e.g. system downtime) [time]
  - Frequency of recovery exercises and tests [number of times per year]
  - Incidents that weren’t identified in risk assessment [number of incidents]
  - Percent of IT services meeting uptime requirements [service level agreement]
  - Percent of successful and timely restoration from backup or alternate media copies [number of systems and times]
Building the Playbook

• Express the required recovery tasks and processes in a manner that provides relevant actions and milestones

• Tactical Phase
  • Execution of the playbook developed as part of the planning efforts.
  • Actions can be organized into initiation, execution, and termination stages.

• Strategic Phase
  • How to reduce the organization’s attack surface and minimize cyber threats.
  • Actions organized into the planning/execution, metrics, and recovery improvement stages.
Example Scenarios of Cyber Events

• Two example scenarios:
  • Exfiltration of personally identifiable information (PII)
  • Ransomware attack

• Scenarios are fictional and not meant to be all-inclusive or exhaustive

• Demonstrates how to apply the document’s recommendations
Questions?