Planning Considerations for Cyber Incidents: Guidance for Emergency Managers – Overview

This resource highlights key concepts from FEMA's **Planning Considerations for Cyber Incidents: Guidance for Emergency Managers.** To review full document, please visit: https://www.fema.gov/emergency-managers/national-preparedness/plan.

Introduction

Nearly all aspects of society rely on networked technologies to communicate and operate. While increased interconnectedness provides better and more efficient services, this ever-expanding reliance on networked technologies may lead to cyber incidents with wide-spread and potentially devastating impacts. FEMA's Planning Considerations for Cyber Incidents: Guidance for Emergency Management is intended to help state, local, tribal, and territorial (SLTT) emergency management personnel prepare for a cyber incident and support the development of a cyber incident response plan or annex.

> Emergency managers are not expected to be technical experts on cyber incidents, but they do need to understand and prepare for the potential impacts of cyber incidents on their communities and emergency operations. Regardless of hazard type, knowing whom to engage during an incident and having plans in place to effectively address an incident's impacts is central to the role of emergency managers.

Cyber Incident Planning Considerations for Emergency Managers

Clearly Identify Roles and Responsibilities

Emergency managers' specific roles and responsibilities in preparing for and responding to a cyber incident may differ from those associated with other incident types. Depending on the jurisdiction, emergency management may take on a lead or supporting coordination role. While it is unlikely that emergency managers would be asked to directly contain or eradicate a cyber threat, it is likely they would be directly involved in the consequence management of an incident. It is critical that emergency managers coordinate with the relevant parties, including their legal advisors, to clearly identify and understand roles. Examples of the potential responsibilities for emergency managers include:

- Prioritizing resources, to include personnel, to address the needs of response and recovery.
- Assisting with communications and notifications.
- Activating other plans (e.g., power outage, distribution management).
- Coordinating with the cyber response team to verify the threat is contained and with stakeholders to ensure that affected operations are restored.

Engage Service Owners & Operators

Owners and operators of critical services and cyber systems provide the most detailed and accurate information regarding system dependencies and vulnerabilities. Additionally, they provide valuable guidance on assessing whether the service remains operational during and following an incident. Engaging owners and operators in the planning process establishes relationships and aids the development of plans, policies, procedures, and protocols.

Assess Cyber Risks

Assessing cyber risks involves identifying the potential cyber disruptions with the greatest impact on a community. These assessments aid in determining the necessary response activities and assists in prioritizing restoration efforts. Assessing cyber risks includes identifying:

- The community's critical services, such as emergency services, water and wastewater systems, and communications, that rely on information technology.
- The interdependencies of critical infrastructure, particularly those related to critical services, cyber assets, and services.
- The consequences of service loss or disruption, with special attention to the problems caused by cyber incidents.

The Critical Cyber Asset Identification and Prioritization Checklist provides a framework for identifying and prioritizing a jurisdiction's critical cyber assets as part of the planning process.

Prioritize & Plan for Disruptions

Once cyber risks, critical services, and dependencies are identified and inventoried, emergency managers determine how vital each cyber asset is for the critical services operating within the jurisdiction. Through ongoing consultation with system owners and operators, emergency managers refine their understanding of what systems are essential, what is required to operate those systems, and what alternative methods are available for operating those services. This information is used to prioritize services, determine how to apply limited resources, and define the order of response efforts prior to an incident.

Provide Integrated Communication & Public Messaging

Communication strategies and the related processes involved for cyber incidents need to be carefully planned in advance. These processes include plans for communicating among emergency management and incident response personnel, as well as messaging to broader stakeholder groups and the general public. Emergency managers consider the following when planning for a cyber incident:

- **Notification of Key Entities:** Which stakeholders to notify, how, and what information to communicate.
- **Reporting:** Whom to contact, (e.g., law enforcement, utilities, DHS/CISA) and what details to report.
- **Alternative Communications Systems:** Backup forms of communication accessible to all relevant stakeholders.
- **Information Sharing:** Processes for sharing information among different responders, including for sharing proprietary or sensitive information.
- **Public Messaging:** Clear procedures for public messaging, including who has primary responsibility for messaging.