Chapter 7
Plans

ABSTRACT

Communities have been planning for disasters for a very long time, especially for natural disasters. The capability to predict when the hurricane will hit a coastal area or island is available. Precautions are reported to the public, and preparedness activities are posted continuously. Planning for cyber incidents is a much newer activity, and it has been getting increasingly more sophisticated as time goes on. A community plans for physical events such as a hurricane, flood, or tornado because they are in geographic areas that are prone to these threats. All communities need to prepare for a cyber incident or attack. In the early 2000s, the CIAS would hear comments such as "Our county is too small" or "No one would target us, we don't have anything they would want." No matter how small the organization and no matter what the size of the community, everyone is a target today. Preparing for "when" the cyber incident happens is the best approach, and that means every municipality, county, and parish should have a plan in place to continue business and to respond to an incident.

INTRODUCTION

Communities have been coming to together for decades to plan and respond to a great number of scenarios that could be harmful or potentially dangerous to the citizens in their community or the business operations of the community. These incidents can occur from natural or human-caused events and require an emergency response to protect life and property.

DOI: 10.4018/978-1-7998-4471-6.ch007

Incidents can include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response to include cyber incidents.

Determining who should respond to an incident will depend on what the incident is and its significance. It is important to note that most incidents are managed at the local level. Emergency plans for a community addresses all-hazard incidents, as previously identified, which typically require a unified response from local agencies, the private sector, and non-government organizations. Some may require additional support from neighboring jurisdictions or state governments. A smaller number of incidents require Federal support or are led by the Federal Government. An important factor for consideration is not all incidents are contained in a specific geographic area. Certain incidents such as a pandemic or a cyber event may span across jurisdictions, states or regions. This type of incident, depending on the nature of it, may be managed at the local, state, tribal, territorial, or Federal level.

BACKGROUND

One of the common findings from the combined results of the Community Cybersecurity Exercises conducted, was there were no plans that included cybersecurity threats and issues. The plans also did not address coordination and response capabilities that focused on cyber incidents. The common misconception was that anything that had to do with cyber was merely an IT problem. This way of thinking does not take into account that a cyber incident could impact an information system that contains critical information needed to provide an essential function. Emergency services are highly dependent on technology and information systems. Services such as computer-aided dispatching for law enforcement and 911 centers, emergency alert systems, event tracking, and monitoring of transportation infrastructure are all very dependent on computer systems that could be disrupted or completely taken off-line due to a denial of service cyberattack.

One of the recommendations from the community exercises was to integrate cybersecurity principles into existing plans and for those who did not have a plan, to create one. Specifically, the recommendation was: