Chapter 1
The Community Cybersecurity Maturity Model (CCSMM)

ABSTRACT

Lessons learned from the community cyber security exercises showed common threads each community needed to focus on in order to improve the community's cyber security posture. These similarities were grouped into four areas of improvement called dimensions. The dimensions are awareness, information sharing, policies, and planning. The methods in which communities can implement improvement are called implementation mechanisms. These mechanisms are common approaches used every day such as establishing metrics, implementing technologies, creating processes and procedures, and conducting training and assessments.

INTRODUCTION

Threats to communities have been traditionally thought of in terms of natural disasters. There have been a number of U.S. cities that have been severely damaged or completely destroyed by natural disaster. Galveston, Texas was hit by a category 4 hurricane in 1900, "destroying nearly 4000 homes, all bridges to the mainland, telegraph lines, most ships in the wharf and even rail lines as far as 6 miles inland" (Crezo, 2012). In 1906, San Francisco, California experienced an earthquake followed by fires. "The initial tremors destroyed the city's water mains, leaving firefighters with no means of combating the growing blaze, which burned for several days and consumed

DOI: 10.4018/978-1-7998-4471-6.ch001

much of the city" (History.com, 2018). The St. Louis Tornado Disaster in 1927, "killed 79 people and caused $1.8 billion dollars in damage (adjusted)" (Crezo, 2012). More recent disasters that should be noted here are Hurricane Katrina in 2005 that flooded 80% of New Orleans after the levees failed, and Superstorm Sandy affecting New Jersey and New York in 2012. Sandy knocked out subway service in New York City and destroyed multi-million-dollar homes at the Jersey Shore. (Harrington, 2018).

These early natural disasters led to the creation of the Federal Emergency Management Agency (FEMA) in 1979. "The Federal Emergency Management Agency coordinates the federal government's role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror" (Fema.gov).

Since FEMA's inception, it has assumed a variety of roles, but it continues to maintain its original mission and over the years has produced many guides to assist communities to prepare for disasters. In 2012, FEMA published a guide called "Threat and Hazard Identification and Risk Assessment Guide: Comprehensive Preparedness Guide (CPG) 201, First Edition". In this guide a table of threats and hazards was provided for jurisdictions to identify the risks most likely to impact their community. Identifying the threats will assist the community to focus preparedness efforts and resources. The risks are categorized into three specific areas:

- Natural – resulting from acts of nature
- Technological – involves accidents or the failures of systems and structures
- Human-caused – caused by the intentional actions of an adversary

Notice in Figure 1, the list of threats has expanded beyond natural disasters. This table represents the recognition that communities potentially face many threats that once were not considered. Cyber incidents are also listed in this table under the human-caused threats. This is significant because it shows the federal government has recognized cyber incidents as a threat a community should prepare for and build capabilities to prevent, protect, mitigate, respond to and recover from.

In May of 2018, the 3rd Edition of the Comprehensive Preparedness Guide (CPG) 201 was published, and the list of example threats expanded and changed the cyber references to "cyber-attack against data" and "cyber-attack against infrastructure" as seen in Table 2. These examples suggest the recognition