Chapter 6
The Two-Dimensional CCSMM

Gregory B. White
CIAS, The University of Texas at San Antonio, USA

Natalie Sjelin
CIAS, The University of Texas at San Antonio, USA

ABSTRACT

The community cyber security maturity model (CCSMM) defines four dimensions and five implementation mechanisms in describing the relative maturity of an organization or an SLTT's cybersecurity program. These are used in defining levels of maturity and the cybersecurity characteristics of an organization or SLTT at each level. In order to progress from one level to the next, a variety of activities should take place, and these are defined in terms of five different mechanisms. In between two levels are a variety of activities that should take place to help the entity to advance from one level to the next. These groups of activities describe four phases, each of which takes place between two levels. Thus, Phase 1 defines the activities that should occur for an entity to advance from Level 1 to Level 2.

INTRODUCTION

The Community Cyber Security Maturity Model (CCSMM) was developed as a result of the lessons learned in conducting state and community cybersecurity exercises around the nation. Exercises are an awareness tool to help people understand the issues related to a specific disaster situation. They are also a proven method to test to see if the mechanisms, processes and procedures an organization has put in place are sufficient to address a variety of different disaster scenarios. With cybersecurity, the issue was first one of awareness – state and community leaders were mostly unaware of the potential impact of a cybersecurity event and needed to be made aware that cybersecurity is an important issue for them. Community leaders needed to understand that without cybersecurity, their community could be negatively impacted in a variety of ways that could cause severe consequences for their citizens. The belief at the time was that by making leaders aware they needed to pay attention to cybersecurity they would then follow up with development of the needed processes, procedures, and technology. The reality proved to be different.

DOI: 10.4018/978-1-6684-3698-1.ch006

When the team that conducted an exercise returned to the state or community to see how well they were doing after about a year, they discovered that while the leaders were still aware that cybersecurity was something they needed to address, they had most often not taken any real steps in forming a strategy to implement a cybersecurity program. There were plenty of vendors willing to sell products and services but which of these were the most important and which needed to be accomplished first before the others? The exercise team had made the incorrect assumption that participants in the exercise would know what to do and that simply did not prove to be the case. They therefore took a step back and created guidance that could be provided to states and communities that would provide a path for them to follow – keeping in mind that most participants did not at the time have a budget to purchase cybersecurity products or services. The resulting plan that was created was the CCSMM.

BACKGROUND

A critical factor in developing the CCSMM was that cybersecurity is not a binary issue. A state or community does not either have security or it doesn't. There are many levels of security preparedness and not every entity needs the same level of security preparedness – it should be based on the actual threats to the state, community, tribe, territory, or organization. This implies there are different levels of security that can be implemented so one of the first tasks in developing a program would be to understand the different levels, understand what is currently implemented, and know what the ultimate goal is. In other words, what security level is needed or desired by the community? The CCSMM was thus created to provide three things:

1. A "yardstick" so that SLTTs could determine where they currently are in the maturity of their cybersecurity program. What level are they currently at? How prepared is the community as a whole, or individual organizations within the community, to prevent, detect, and respond to and recover from a cyber-attack? At first the critical infrastructures in the community and the local government entities will be the primary components the model will focus on but as the community matures, it will increasingly take on a whole-community approach. There are several dimensions that will be described and a community may not be at the same level for all dimensions at the same time. In fact, it is will not be uncommon for a community to be at several different levels among the dimensions as it progresses. To be considered at a specific level overall, however, the community has to exhibit the characteristics in all of the dimensions at that level.
2. A "roadmap" to describe a path to advance from one level to the next. This would describe the various activities that need to take place in order to advance. After determining what level the community currently is at, a decision needs to be made concerning what level they aspire to. Not all communities are the same and not all communities will need to attain the highest level of security represented in the model. The level of threat to a community will be heavily dependent on what organizations reside in the community. For example, is there a military installation or a large component of the federal or state government? Is there a significant national monument or historical site that serves as a symbol for the nation? Is there a significant industry or manufacturing installation present in the community? All of these will impact the likelihood of an attack on the community as well as the potential threat actor (i.e. who might want to launch an attack on the community or organizations within the community – a nation-state, a criminal organization, a