Chapter 10
Incorporating Other Models and Technology Into the CCSMM

ABSTRACT

One thing about the nature of computer science in general and cybersecurity in particular is that they are both fields that are constantly changing. Whether it is because of a new version of an operating system being released, new technology that has been introduced, or a disclosure of a newly discovered vulnerability, the field is continually changing. Some changes will not have any impact on the CCSMM. Others may necessitate a change in some aspect at one or more levels. The model itself is extremely flexible and frequently does not specify the precise items that need to be covered but rather the more abstract concept that must be considered. This is true for not just changes in technology but also the introduction of new government guidance or regulations as well as the creation of other maturity models that are focused on some other aspect of cybersecurity. This chapter explores incorporating other models and technology into the CCSMM.

INTRODUCTION

The creation of the CCSMM came about after years of dealing with SLTTs and assisting in the development of their security programs. Those years were certainly not static in that what was accomplished in the early years was not

DOI: 10.4018/978-1-7998-4471-6.ch010

exactly the same as what occurred in later years. This was due to a number of factors including the introduction of new technology, regulations, federal guidance or the discovery of new vulnerabilities in software or hardware. As the model was developed, the fact that for the model to remain applicable it would need to be flexible enough to allow for these types of changes was recognized and planned for. Fortunately, when considering the community scope this is easily accommodated. For the organizational scope you will find that the requirements at each level are much more technologically specific. Instead of a general statement stating that organizations in the community need to institute some form of asset management that keeps track of hardware and software (which might be a requirement for the community scope), for the organizational scope the requirement might be for one organization to implement inventory control based on NIST SP 800-53 Rev 4, CM-8, PM-4 while another utilizes ISA 62443-2-1:2009 4.2.3.4. Since this book covers the community scope, how to address the inclusion of new technology, regulations and guidance, and other models into the CCSMM will be covered in this chapter.

BACKGROUND

The CCSMM addresses multiple ranges (or scopes) of entities. From individual citizens to the entire nation the CCSMM describes the characteristics and activities that define five different levels of maturity for security programs. This book addresses the CCSMM at the community scope. A community will consist of several different types of organizations with varying specific security requirements. Banks fall under different federal security regulations than do hospitals, for example. From a higher perspective, however, both have similar security requirements. Should one of the regulations change a specific requirement, it does not negate the usefulness of the CCSMM for the community. What it does is change an organizational requirement for entities that fall under that regulation. The overall CCSMM model would remain unchanged.

Another area in which change may occur necessitating changes in the various implementation mechanisms is technology. As new technology becomes available it will often introduce different security vulnerabilities while at the same time eliminating others. A good example of this is the switch from