Chapter 3
The NIST Cybersecurity Framework

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

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

ABSTRACT

With the increase in cybercrimes over the last few years, a growing realization for the need for cybersecurity has begun to be recognized by the nation. Unfortunately, being aware that cybersecurity is something you need to worry about and knowing what steps to take are two different things entirely. In the United States, the National Institute of Standards and Technology (NIST) developed the Cyber Security Framework (CSF) to assist critical infrastructures in determining what they need in order to secure their computer systems and networks. While aimed at organizations, much of the guidance provided by the CSF, especially the basic functions it identifies, are also valuable for communities attempting to put together a community cybersecurity program.

INTRODUCTION

It is a common problem among individuals attempting to secure an organization's critical computer systems and networks to struggle with where to begin. With limited budgets, where can the funds be used most wisely? Can an incremental plan be developed to ultimately arrive at the security posture desired but over a period of time that takes into consideration the need to work within budgets?

The CCSMM introduced in this text is a plan to help guide communities in the creation and maturation of their cybersecurity program. A geographic community, however, is made up of a number of organizations and individuals all of whom will contribute to the security, or insecurity, of the community. This text focuses on the overall community's program and does not delve deeply into a plan for any one type of organization or sector. This is where the NIST Cyber Security Framework (CSF) enters the picture.

DOI: 10.4018/978-1-6684-3698-1.ch003

The CSF was designed to provide guidance to the critical infrastructures on how to organize their security efforts based on a plan to manage cybersecurity risk in a cost-effective way.

The CSF contains a lot of great information and guidance. Unfortunately for many organizations, in particular smaller organizations, the amount of information contained in the CSF can be overwhelming leaving people in a similar position to where they were before reading the CSF. Recognizing this, NIST produced another document, *Small Business Information Security: The Fundamentals*, which discusses much of what is introduced in the basic core of the CSF without the overwhelming list of sub-categories and references that the CSF contains. This allows small businesses to focus their efforts in an organized manner as they go about securing their systems and networks.

For communities, the CSF also contains much information that will not be immediately useable at the community level although it will pertain to many of the individual organizations within the community. Instead, the topics introduced in the companion document for small businesses that NIST produced can help focus a community's efforts providing an extra level of guidance that will enable the community to organize their efforts. Thus, the CCSMM and the CSF can go hand-in-hand within a community to help the community address cybersecurity from different angles.

BACKGROUND

Since the 1990's, the federal government has been keenly aware of the dangers cyber events posed to the various critical infrastructures and thus focused considerable attention on securing these infrastructures. PDD 63 issued in 1998 and discussed earlier in the text was a big step forward in organizing the efforts of the various critical infrastructure sectors so that they could collectively work together to solve the challenges they each faced. Then in 2013 the White House issued Executive Order 13636 (2013) *Improving Critical Infrastructure Cybersecurity* which continued the focus on the critical infrastructures and attempted to keep things moving in a direction that would lead to more secure infrastructures. Besides addressing information sharing as was discussed in a previous chapter, EO 13636 also directed NIST to "lead the development of a framework to reduce cyber risks to critical infrastructure."

In 2014 the Cybersecurity Enhancement Act (CEA) of 2014 was signed into law. One of the things that this act did was to expand the role of NIST to "identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks". (CEA, 2014) This in essence expanded upon the previous guidance in EO 13636 provided additional guidance to NIST for the creation of a framework.

In 2014 NIST released version 1.0 of the *Framework for Improving Critical Infrastructure Cybersecurity*. In 2016 revision 1 of the *Small Business Information Security: The Fundamentals* document was released which incorporated much of the basic framework from the CSF but made it more useable for small businesses. In 2017 a draft of CSF version 1.1 was released for public comment and in April of 2018 version 1.1 was officially released. This new version was compatible with the original in that it did not change the basic framework but instead expanded upon it to take into account things outside of the critical infrastructures such as their supply chains.

NIST and the federal government have been encouraging not only the critical infrastructures but government agencies to adopt the framework as part of their cybersecurity programs. They have also encouraged industry to use it as well and several large government contractors have done so and pub-