Chapter 9
Building Your Community Cybersecurity Program

ABSTRACT

Communities and states are targets of cyber-attacks. Cities are popular because of generally lax cybersecurity postures and the fact that they have money. States and communities also have personal information on citizens, which can be used for identity theft. With the realization they are becoming frequent targets, communities are looking to enhance their cybersecurity programs, but many do not know where or how to start. The community cyber security maturity model is designed for this purpose – to help states and communities to develop their own viable and sustainable cybersecurity programs. There has also been considerable media attention on the NIST Cyber Security Framework. This is a program designed for organizations, and it contains a lot of good information organizations can use to enhance their cybersecurity posture. From a whole community perspective, however, it is not as useful though there are parts of it that are applicable to a community.

INTRODUCTION

Communities need cybersecurity programs. This means not just for the city government and the critical infrastructures but for all members of the community. Citizens of the community may frequent a variety of stores where they may provide their credit card information. This information is going to be used and may be stored for the logging of transactions. In most

DOI: 10.4018/978-1-7998-4471-6.ch009

communities, especially larger ones, there will also be a number of small doctor and dentist offices that have personnel health information about their patients. It is of interest to the citizens in the community that all of this information maintained by local businesses and offices follow cybersecurity and privacy best practices so that personal information is stored and transmitted securely. In addition, the businesses themselves are interested in protecting their computers and networks because they do not want to suffer a loss from a security breach or from other types of attack such as ransomware. Basically, cities and the businesses within them are becoming increasingly interested in cybersecurity. Knowing what to do in order to start a cybersecurity program within a community or to enhance an existing one is not immediately obvious. There is a plethora of vendors and service providers with tools and services that they will be willing to sell to the community and organizations within the community, but is what they are offering the right tool or service for what the organization or community needs at that time? The CCSMM provides a way to measure the current status of a community's cybersecurity program and a path for the community to follow to improve their cybersecurity posture. In its four dimensions and its five levels it provides a model for organizations and communities to follow that will also address the five functions essential to a cybersecurity program that forms the basis of the NIST Cyber Security Framework – namely Identify, Protect, Detect, Respond and Recover.

BACKGROUND

The Department of Homeland Security (DHS) has been producing the National Preparedness Report every year since 2012. This report provides a lot of interesting information regarding the nation's level of preparedness from a state perspective. Part of the report is an assessment by the states themselves as to how prepared they feel they are in a variety of areas such as Mass Search and Rescue Operations, Public Information & Warning, Fire Management and Suppression, and Health and Human Services. The diagram below shows the results for the 2017 report. This report grouped the information in a format where it is easy to see a comparison between the different disciplines. The 2018 report split the disciplines up so that there was no single chart that presented a quick way to compare the disciplines. The numbers for cybersecurity, and the placement of it in comparison to other disciplines, however, remained fairly steady – thus the reason the chart from 2017 is utilized here to illustrate the point that states are not prepared