Chapter 5
Information Sharing

ABSTRACT

From the first community cybersecurity exercise the CIAS at UTSA conducted in San Antonio in 2002, information sharing has been a key element of the community cybersecurity program. Information sharing is essential in the protection and detection aspects of programs such as the NIST cyber security framework. Information sharing helps to alert other organizations to ongoing reconnaissance and attack efforts by attackers. When it comes to cybersecurity, organizations are not in competition with each other but instead are partners in a mutual defense against attackers. This has not been an easy lesson to learn, and it has taken time, but today, there are many robust information sharing programs that help various sectors and geographic regions to band together to help each other in efforts to thwart attacks against any member of the group. Information sharing is an integral part of the community cyber security maturity model and can in fact help provide a catalyst to launch an overall cybersecurity program for a community.

INTRODUCTION

A question often asked is "why would I want to share information with others? Especially my competitors?" This is a natural question that comes up when an individual is approached and asked if they want to participate in an information sharing program. As an answer to this, consider the following comment:

DOI: 10.4018/978-1-7998-4471-6.ch005

Learning from the mistakes of others sounds great. Yet it's difficult to do when those 'others' refuse to be transparent about their mistakes.

Why is intelligence sharing important? Cyber criminals find new software vulnerabilities and attack vectors every day. Cybersecurity experts are faced with an ongoing challenge to keep up. If peers open up to proactively share information–also known as [information] sharing–it can help strengthen our collective resilience and reactivity to potential threats. (Red Team, 2016)

This short quote from a 2016 blog highlights two points. First, people are often reluctant to share information with others which makes "learning from the mistakes of others" or maybe more importantly "learning from the current events impacting others" difficult to impossible. People are reluctant to share for a variety of reasons, the prime one being a concern about how the information they share will be used by others. Will providing information on a breach in one company be used by a competitor in a marketing campaign highlighting the past security problem of the first? Another issue is that of the privacy of the company and its customers. Both, however, have successfully been dealt with by information sharing organizations and it just takes some time for a new organization to trust that sharing information will not be detrimental to them.

The second point highlighted by the quote from the blog states that intelligence sharing (or information sharing) is important because of the "ongoing challenge to keep up" with cyber criminals that cybersecurity experts face. New vulnerabilities and attack vectors are discovered on a frequent basis and it is often hard for a cybersecurity professional to wade through the plethora of information presented to determine what is important to the organization. Frequently it seems like the criminal (or "hacker") community does a better job of sharing information than cybersecurity defenders.

In this chapter the topic of information sharing as it relates to a community will be discussed and the plan to implement cybersecurity information sharing within a community at the different levels of the CCSMM will be presented. It is stressed throughout this book that there is no single perfect description or plan for a community hoping to develop a viable and sustainable cybersecurity program. What will be presented in this chapter will be higher level constructs with some suggested specifics, but specific approaches must be adapted to individual communities and their local environment.