INFORMATION SHARING SELF ASSESSMENT

Information Sharing Self Assessment Introduction

When cyber events affect our organizations and communities, sharing information about these events may be required or prove beneficial. Moreover, being aware of cyber events occurring elsewhere may help us take precautionary steps to limit their effects.

The goal of this document is to provide a framework for identifying current and desired information sharing partners, delivery methods, frequency and other considerations associated with an information sharing program. It is intended that this document be used as a planning tool for building or enhancing information sharing policies and procedures. As such it is not intended to be a comprehensive list.

The layout is designed to help organizations walkthrough the steps involved in creating a comprehensive information sharing program. It contains a list of high-level topics that address specific instances in which information sharing may be warranted. Following the listing of those topics are worksheets that can help analyze gaps that may exist in the information sharing program.

For each high-level topic, organizations can determine the information that should be shared by them and the information that should be shared with them. An organization can then use the current state assessment worksheets to determine where gaps exist in both the incoming and outgoing information sharing processes. The gap list can then serve as a roadmap for improving or creating information sharing policies and procedures.

Sample High Level Topics

As different situations may require different methods of sharing information, these example high-level topics can be used as a basis of potential situations for planning purposes. By applying the following checklist to these high-level topics, organizations can build or enhance their information sharing strategies.

- Intelligence and discovery
- Security breech or compromise
- Third party incident or compromise
- Virus or worm outbreak
- Incident requiring third party assistance (such as Distributed Denial of Service)
- Extortion
- Physical theft of IT Assets
- Loss of personal data (employee/customer)
- Child pornography
- Solutions and lessons learned (post mortems)
- Other