Maritime Transportation System Information Sharing and Analysis Organization: Charleston
MTS-ISAO: Charleston

SITUATION

Cyber threats are increasing at an alarming rate. Recent reports indicate that the number of data records taken from companies more than doubled in 2016, and while the majority of cyber crime is financially motivated, attacks with a political or terrorist motivation are growing. Recently a confidential report from MARAD identified a ransomware attack (malicious software that encrypts computers until a ransom is paid) to multiple systems on a U.S. ship, and there are increasing reports of cyberattacks on ICS platforms in many industries.

Charleston is very strategic from both a commercial and military standpoint, ranked eighth in the US for container volume and home to multiple military transportation units. South Carolina is in a natural position to lead in developing cyber community defenses to protect these assets.

RESPONSE

While every organization must provide their own cyber defenses, community defense - where entities with a common interest band together to share information about observed threats and responses - are growing. These communities, called ISAOs, were enabled by legislation and presidential directive.

MASC is proposing such an organization to improve the cyber defense of South Carolina's maritime sector and the related transportation community. Grant funding is being pursued to support the start-up, and the vision is for the community to become self-sustaining as it matures.

OPERATIONS

The organization will focus on community education, preparedness and intelligence sharing. A board will be formed to guide the direction and development of the ISAO, and part time Executive Director services will be provided by Gate15 Global Consulting. The ISAO will operate initially as part of MASC. Gate15 provides similar services to a number of other sharing communities now.

Meetings and calls on the cyber landscape, preparedness, education and information sharing will be held, along with emergency response calls as needed. The ISAO will also maintain relationships with other intelligence groups and government agencies such as the USCG, NMIO and MARAD.

TOOLS

Two tools lend themselves to this effort:

HiveIQ from Teamworx – a secure collaboration tool that allows analysts or dedicated IT staff at member companies to assess and respond to threats in real time.

Perch Security – a sensor and cloud-based application providing network activity monitoring, threat assessment, and corrective action communicated in near real time to companies without dedicated security staff or significant security resources.

Initially the cost of these tools is expected to be covered by grant funding, which can be replaced over time with individual company or individual grant funding.

MEMBER BENEFITS

By joining a cyber-intelligence sharing community, members will be able to increase their awareness of cyber-threats as well as potential breaches to their network. This heightened sense of situational awareness can also be shared with the rest of the membership, improving the cyber security posture of the entire community, as well as their readiness to respond in the case of an event.

Prime contractors are beginning to examine the cyber security capabilities of their supply chains, so an active cyber security stance will be necessary to do business.

This improved security posture will be a differentiator for the Port of Charleston and can be a factor in continuing to win competitive port business.