Insights

By Greg Girard

Maritime ISAC
A Glass Half Full

There is always someone who can benefit from information you are willing to share. Sharing information that will help others almost sounds like the second Golden Rule, or at least a simple moral we would teach our children. But can this same simple rule apply to a "real world" maritime scenario?

As a backdrop for the information to be shared, let's add drug trafficking, crime syndicates, terrorist plots, national security implications, advanced military technology and weaponry, seas that cover 70 percent of the world's surface, 90 percent of the world's cargo, marauding pirates, governmental sovereignty, agency jurisdictions, multi-million dollar corporate losses, and legal liabilities. Is it then so easy to apply our second Golden Rule? It certainly is necessary, but it can get a bit more complicated.

This backdrop is unfortunately the current status of the maritime environment, and while sharing information plays a role in the overall national maritime security structure, it often gets lost in the race for higher fences, more grant allocations and the latest and supposedly greatest technologies.

INFORMATION SHARING

An essential component to security within any transportation or critical infrastructure sector is intelligence. Accurate and timely information can prevent, deter and discover all forms of criminal and terrorist activity and is the true foundation of any proactive security philosophy.

It is understandable then that in 1998, a Presidential Directive (PDD 63) was published calling for a "national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures" and stating that "Information Sharing and Analysis Centers (ISACs) are encouraged to be set up by the private sector in cooperation with Federal government."

Over the years, this idea of information sharing with the private sector has been reinforced by numerous government documents and testimonies. As an example, in 2006, An Information Sharing Environment Implementation Plan, written by the Information Sharing Environment Office and the Information Sharing Council, noted "private sector information represents a crucial element in both understanding the current threat environment and protecting our nation's critical infrastructure from targeted attacks."

Several industries, prompted by these overt calls for collaboration by government, began establishing various critical infrastructure ISACs. Indeed, in 2003 the National Council of ISACs was founded, providing 16 active ISAC organizations with a forum for collaboration between both the critical infrastructures themselves and their respective government partners.

While the concept of ISACs is accepted as sound and both government and industry are cognizant of the potential benefits, obstacles remain. Three issues stand out:

• **Information overload:** Noted American physicist William Pollard said, "Information is a source of learning. But unless it is organized, processed and available to the right people for decision making, it is a burden, not a benefit." We are truly suffering from information fatigue. There is so much information, coming from so many sources, that it often becomes a detriment rather than a benefit to those trying to use it.

• **Ambiguous lines of communication:** While sharing the information is half the battle, recognizing who can best use the information is the other half. Where can I get the information I need? How will the information I share be used? These questions rarely have a definitive answer, particularly when faced with ever evolving rotations within government agencies. A familiar, and frustrating, scenario is industry representatives working for months and years establishing relationships with agency contacts only to have those contacts rotate out to another agency or office with their replacement having no background on the prior relationship established. This "treadmill collaboration", where relationships can't get to that next level of trust, can only negatively impact proper cooperation in the event of a terrorist act or crime.

• **Commitment Issues:** Sharing is a matter of trust. It is understood that government and industry cooperation is essential to properly securing critical infrastructures. What is difficult to achieve is how both parties get over their apprehension of trust. Government, rightfully so, needs consistent reassurance that the information they share will only go to those who have been properly vetted. And industry, rightful-

ly so, must be assured that the information they provide will not be used against them.

Essentially, these issues are exactly why ISACs were proposed: Industry will create a valid and important layer within the national security structure that can distill redundant and superfluous information flowing between government and industry through expert analysis; provide a centralized repository of information that can maintain sustained lines of communication; and work as a trusted agent between government and industry, assuring both confidentiality and anonymity.

ISAC FOR THE MARITIME ENVIRONMENT

It should be surprising therefore that despite the general understanding and acceptance throughout the maritime community that prevention is more operationally effective than response and recovery, the maritime industry does not yet have a reliable, comprehensive information sharing network. There is hesitation on both sides – some warranted, but most seems just territorial. Admittedly, maritime transportation is a unique industry. It is international in scope, its boundaries are malleable and its impact on the global economy is unparalleled. There is more information to digest and more risk of information getting into the wrong hands. All the more reason to establish stronger bonds of cooperation and collaboration between industry and government … there is so much more to lose.

While the Maritime Security Council does indeed serve as a de facto Maritime ISAC, gathering information from open sources, analyzing specific maritime security issues, distributing the information to its membership, and representing the maritime industry as a member of the National Council of ISACs, much more needs to be done. The maritime industry needs an ISAC with complete government support. This "full service" Maritime ISAC will handle sensitive security information; provide real-time analytical support during incidents; offer trusted lines of communication; maintain a database of worldwide port conditions; and analyze – in a secure environment – information gathered from all interested parties.

Publilius Syrus, a writer from the 1st century BC wrote, "Anyone can hold the helm when the sea is calm" and I would suggest that an addendum to the quote could read "but it is when the sea is restless that those most prepared will find safety." It is time for a "full service" Maritime ISAC.

The Author

Greg Girard is Vice President of Communications & Operations for the Maritime Security Council and has worked in the international maritime security sector for the last decade. He is editor of the Maritime Information Sharing & Analysis Center (Maritime ISAC) Alert, an open source and analytical report distributed twice weekly to the MSC membership.