Maritime Cybersecurity More Important Than Ever, But Industry Only Talks About It

Posted to Technology January 28, 2019 by Kate Patrick

Feds and private sector leaders in the maritime industry met in last December to discuss cyber risks, but instead of making serious progress, the results were, as one expert put it, “like standing around a building that’s on fire and talking about the infrastructure.”

According to a new report provided to InsideSources, the National Maritime Intelligence-Integration Office (NMIIO) and the National Strategic Research Institute (NSRI) are in the middle of a study on cyber risks in the maritime industry, spanning February 2018 to August 2019, which will be presented to the Director of National Intelligence and the National Security Council.

Cybersecurity is a serious issue for maritime industries. Major ocean carriers like Maersk and COSCO and ports like the Port of Los Angeles and the Port of San Diego suffered severe cyberattacks over the last few years, temporarily crippling their supply chains and, in some cases, bringing the flow of goods to a halt.

Interested parties from both government and industry participated in a December workshop to evaluate current cyber challenges in maritime. But a report of the workshop summarized by the NSRI shows they skirted around the real issues and instead focused on coordinating responsibilities and information-sharing strategies.

In other words, they talked about getting work done, but didn’t do any work.

It wasn’t a total waste, however: workshop participants agreed that the entire maritime supply chain should be up to date on cyber risks and cybersecurity initiatives, and determined that the biggest cyber risk within the maritime supply chain is third party vendors, like contractors and software providers.

In order for the maritime industry to really crack down on cybercrime, every link of the supply chain must augment its cybersecurity. But that’s an obvious observation, said James Rice, deputy director of the Massachusetts Institute of Technology’s Center for Transportation and Logistics.

“They wanted to understand the environment for the industry,” he told InsideSources. “Okay yeah, but that’s like standing around a building that’s on fire and talking about the infrastructure.”

One way to mitigate cybercrime is via information-sharing between the attacked entities and others within its supply chain. Information-sharing is standard operating procedure from a cybersecurity standpoint, and while it may conflict with privacy initiatives for industries dealing directly with consumers, within the maritime industry it makes sense.

But there’s currently no straightforward way to do that, the report noted.

https://www.insidesources.com/maritime-cybersecurity-more-important-than-ever-but-industry-only-talks-about-it/
According to the report, “there is general consensus on two main points: 1. An Information Sharing & Analysis Center (ISAC) dedicated to maritime issues is beneficial because an ISAC provides anonymity to reporting entities, provides analytic horsepower to correlate events across the industry, and coordinates with appropriate government organizations to provide a bridge between industry and government. 2. There is need for clear and consistent direction on dissemination and reporting requirements/capability.”

It appears the maritime industry’s view is that more bureaucracy could streamline cybersecurity efforts. In Rice’s view, this just shows how badly prepared U.S. infrastructure is for cybercrime.

“The state of cyber resilience is one where people are aware of the issues, but performance is, what should we do about it? And I think if they were further along we’d see more discussion about vulnerability assessment and how to deal with problems then, what’s the environment?” he said.

https://www.insidesources.com/maritime-cybersecurity-more-important-than-ever-but-industry-only-talks-about-it/