Superyacht cyber resilience

Do superyacht owners understand the importance of cyber resilience?

February 11, 2019

Joe Hollier IV is an insurance specialist in Cyber Risk for Alliance Insurance

If I were to run to the bow of a vessel and scream into the ocean air, it would sound a bit like this: "Know your cyber vulnerabilities! I repeat, know your cyber vulnerabilities!" While likely that may draw strange looks, a more simplified context would reiterate - get a better understanding of how hackers are trying to steal from you and completely shut you down.

Superyacht owners are quickly learning of the immediate need of a cyber resilient strategy. They may not know to refer to it as cyber resilience, but most know to some degree the significantly damaging effect that hackers and cyber criminals can impose on the information and operation technology of the ship. By significantly damaging I mean very, very costly. People are part of the problem not the solution.

In a conversation with Itai Sela, CEO of maritime cyber defense company Naval Dome, this is the statement that truly grabbed my attention.

"In the end people will make mistakes," says Sela, therefore a more advanced, secure strategy would involve removing the human touch elements. The numbers are staggering. Not just in the maritime industry but across multiple industries. By 2018 estimates, 90 per cent of cyber attacks in the US are a result of human error. New approaches to minimize the "human factor" are ongoing with many tech developers, and such is the case with the product system by Naval Dome. As Sela explains, "our cyber defense dashboard protects the two channels of IT and OT without the network interference of crew or staff. When ND Endpoint technology is installed on two PC-based systems, all communications between them are cyber secured." Zero human touch, more secure system.

"Superyacht owners are quickly learning of the immediate need of a cyber resilient strategy." Sela goes on to remind me however, "no system is 100 per cent secure." Note there is a sentiment that should never be ignored. No level of security is absolute in the ever-changing malicious hacker landscape.

Cyber Insurance is evolving in the wake of CL 380. This is welcoming news, as the trend in insurance liability coverage since the words cyber and loss were forced together is that insurance carriers will not cover any losses due to the use of any computer, computer system or software program, as so intentionally stated in the highly unpopular CL 380 exclusion clause. In short, the CL 380 excludes all things cyber-related. Much to the dismay of many in the maritime industry, there has been much movement to have the clause revoked, including the efforts of Mr. Sela as recently as last fall. The CL 380 still remains.

However, where there is demand there is opportunity. Addressing the most pressing of cyber-
related gaps in insurance coverage has spawned aggressive action from policy developers and carriers. Much like the technology to prevent intrusion and attacks continues to reiterate, so has the cyber liability insurance policy, as carriers are specifically crafting forms and policies around the detailed exposures of their target market.

An important thought to close on is the reminder that cyber criminals are not a one trick pony. Just as tech companies and insurance carriers are feverishly working on ways to prevent and protect against cyber destruction, hackers are also committed to finding new ways around the wall.

As it stands, a majority of superyacht owners only currently have one firewall between their networks and a malicious actor. This is enough to make me want to scream from the bow.