Marine cyber threat causing problems for t’s & c’s

By Insurance Marine News, 9th July 2018

Participants in a panel at Marine Insurance London 2018, held on Thursday July 5th, warned that the risks posed by emerging cyber threats were such that both Lloyd’s and the Prudential Regulatory Authority (PRA) were pressing for Cyber Attack Exclusion Clause 380 to be extended to include non-malicious attack. That clause reads:

“in no case shall this insurance cover loss damage liability or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system”.

On the same panel one participant said that aggregation risks were such that he did not think single insurers could tackle the problem alone, that some kind of pool insurer might be needed.

The panel, chaired by freelance journalist Ant Gould, consisted of Andrew Hannay, Senior underwriter Norwegian hull; Charles Fernandez, head of marine liability and hull at Canopius, Giles Hunnisett, master mariner and consultant with Waves Group, and Monica Tigleanu, Partner, Cyber, JLT Specialty:

Hunnisett observed two significant cyber-related risks – the removal of traditional paper charts and the reliance on ECDIS; and the black box which is connected to ECDIS which pulls in information from all over the ship. Hunnisett said that this was a risk for a single ship, but he warned that there were greater problems. “What I am looking at more and more is a more widespread problem. ECDIS could have 20,000 vessels, all of them updated by a few companies. Imagine a bug getting into 1,000 ships all at the same time. These would not be able to leave or enter ports, or, if they were at sea, know where are. The consequence would be huge business interruption and, quite possibly, crashes. The more people I see the more I hear that they are surprised it hasn’t happened yet. Meanwhile, on board, we know the danger, but we can’t do anything about it”, he said.

Charles Fernandez observed that cyber risks could be broadly put into three categories:

1) Physical loss or damage

2) Business interruption which is not necessarily a loss of physical damage

3) Loss of theft of data by third parties. Cost of reconstitution computers.

The question was, where would these risks be insured, in the marine market or in the cyber market? He said that physical loss should probably go to the marine market, while loss of data should go to the cyber market, because that would be where the expertise lay in those particular risks.

Fernandez also noted that the insurance of cyber risk in marine, and elsewhere, had challenges of pricing and of aggregation. To price a product, one needed to be able to estimate probability and severity. “And at the moment we can’t answer those questions”. He said that insurers needed to interact more with experts in order to price products properly.

However, Fernandez saw aggregation as an even bigger danger. “Just 100 to 200 ships affected by the same event could lead to huge aggregation risks. This could be dealt with by maybe a pooling or consortium arrangement. But I don’t think insurers can attack that alone.”

Monica Tigleanu said that JLT’s clients consistently said that they were relying on information systems to generate top and bottom line, which meant that cyber was no longer really an ancillary risk. Last year’s Maersk incident convinced many clients that a cyber-attack did not have to cause physical damage, while generally the larger clients were most concerned with state sabotage.

She also noted that the issue on the insurance side was who wanted to cover what. Although aggregation was a problem for insurers, it was not something that clients were particularly interested in. What they wanted to know was. what would they be covered for under their policy.

At this point Andrew Hannay observed that from a shipowners’ perspective the buyer would be happy to delete clause 380 from the policy, but the question was, what would happen when it all went wrong. How would the insurers respond?

Fernandez observed that it was a recipe for disasters. Shipowners did not understand their cyber exposure, and, while insurers understood the aggregation issue. There was a creeping in of exclusion clauses being deleted. “If insurers are providing the (cyber) cover, it should be clear how they are covering it, because the aggregation losses could be huge”, he said.

Hannay noted that Clause 380 was in the position of being reviewed and extended. At the moment it referred only to a malicious attack, not a non-malicious failure. The PRA and Lloyd’s were putting pressure on insurers to exclude by default both malicious and non-malicious cyber events. But he said that just introducing a new exclusion clause was not a solution, given the type of risk cover now required by clients.

All participants agreed that part of the problem was that looking backwards was not particularly helpful, because the cyber landscape was continuously changing. This caused problems for clients because they did not know where the next attack was coming from, and for insurers because they did not want to cover “everything” when they could not know how severe and with what consequences a future attack could be. Hannay said that cyber policies were selling well, but insurers were not willing to offer high limits and wide cover, because of the aggregation problem. Meanwhile Tigleanu said that JLT’s clients did not want off-the-shelf products. It was the ability of insurers to offer products suited to particular clients that would make the difference.

This article is kindly supplied by Insurance Marine News. If you would like a complimentary trial to the daily Insurance Marine News e-bulletin please email grant.attwell@insurancemarinenews.com.