Insurance Marine News

Loss prevention the source of technical result improvement – Dubois

By admin On September 15, 2021 In Cargo, Insurance Marine News, Keep, Marine Hull, Marine Liability

IUMI Blog – Day 9

As the International Union of Marine Insurance headed towards a close today, Pascal Dubois, (Managing Director, General Management, CESAM, FR-Paris), said in his chairperson's report for the Loss Prevention Committee that his credo was "loss prevention as a source of technical results improvement. He noted that loss prevention had two unique aspects. The first was that it was the only thing that was under the total control of insurance companies when it came to influencing the bottom line. And the second was that there was a virtuous circle when it came to loss prevention, starting with teamwork and finishing with better profits.

In a roundtable moderated by Howard Potter (Head of Underwriting, Underwriting, Astaara, UW – Astaara), to discuss cyber security and how losses could be prevented, the panellists were asked what the main cyber risks were.

May Jensen (Director Risk Management, The CSL Group Inc.) said that first and foremost in her mind were people. She said that, when humans were involved, there was always a danger that something undesirable would happen.

Vincent Lagny (Chairman, Cyber Panel, IACS (International Association of Classification Societies)) said that several attacks relied on the interconnectivity of networks, network vulnerability and human error.

Lagny had something of an apocalyptic view of the cyber threat. He said that it was unrealistic to think that cyber-attacks would not happen. And, when they did, they would probably impact several vessels at the same time.

Philip Ponsford (Deputy Chief Cyber Officer, Astaara Risk Management, Astaara), said that from a seafarer's point of view the most likely points of attack would be the areas easiest to get into – i.e., financial details. But the most threatening would be if attackers got into systems involving the ship's safety. But Ponsford was somewhat optimistic. He said that much could be mitigated by the use of back-up systems. Seasoned professionals

knew how to transfer over to back-ups. They also know to look out of the window rather than rely solely on electronic indicators.

Ponsford's view was that most disasters at sea were the result of a series of errors and failures laid end to end. He thought that a cyber-attack would cause a disaster only if it were part of such a sequence. In other words, a cyber-attack could weaken resilience. If linked to other events, and if there were an inexperienced crew, then there could be a major event. "But it's hard to imagine a seasoned crew being unable to intervene if there is an attack", Ponsford said.

He observed that 95% of cyber events were the result of people not following procedure. So, the answer is, don't let people charge their mobile phones in sockets connected to ship software. Don't let them insert USBs.

Kevin K. Adams (Marine Transportation System Cybersecurity Specialist, Prevention / Investigations & Inspections, United States Coast Guard, First District, USA-Boston) said that at the USCG they tried to take a holistic approach. Taking something of a high-level view, Adams said that it was important for the chief information officer to be at board level and to be able to argue why the budgeting was needed to protect against cyber-attacks.

He related one incident this year where five vessels saw their corporate network hit, rather than individual ships. This meant that their operational technology (which was working fine) could not communicate with the IT of the company on sure. "We got the five boats to safety, but when we got on board, we discovered that there was a greater risk than anyone realized", warned Adams.