TradeWinds
The Global Shipping News Source

ALEXANDER SOUKHANOV: At the CMA conference.
Photo: Chris Preovolos

Shipping struggles to come to grips with cyber security threat

As the global industry becomes more digital, the risk of attack or accident grows

March 23rd, 2017 18:00 GMT by Eric Martin Stamford
Published in WEEKLY

A modern ship, outfitted to the brim with digital technology that made it paperless, suffered a failure of its navigation software because of a computer virus while in port. The problem prevented it from sailing for five days.

As the industry begins to embrace digital technology, and as more networked systems are integrated into vessels, so the risk grows of breaches in cyber security and incidents like this one causing ships costly delay.

Shipping experts speaking to TradeWinds on the sidelines of the Connecticut Maritime Association (CMA)'s Shipping 2017 conference say the principal cyber risk is not the doomsday scenario in which hackers take control of a vessel and threaten to take it off course and into harm's way (although they do not deny that this is a remote possibility).

Instead, they point to mounting evidence of real incidents in which ships'

operational systems have been compromised by digital threats such as malware and viruses inadvertently introduced by crew.

Captain Alexander Soukhanov, director of maritime cyber assurance research at the non-profit US Maritime Resource Center (USMRC), says the industry's awareness of cyber security is increasing more slowly than it should be. Cruise lines and the offshore sector are ahead of the curve, but bulkers, containerships and tankers are lagging behind.

"They know cyber is out there. Are they doing anything about it? I would say no," said Sean Kline, director of maritime affairs for the Chamber of Shipping of America.

Among the real-world examples, there have been several situations in which vessels have been prevented from sailing because of viruses in their navigation software. In at least one case, the situation was caused by a crew member who charged his mobile phone in its Actis navigational computer.

One ship has suffered the impact of computer viruses that were dormant until a particular piece of equipment was connected to the internet for some time.

Another vessel was besieged by malware two hours after an engineer searched a seemingly legitimate online catalogue, minimising a pop-up window without realising it would unleash problems.

Even when shipowners isolate a vessel's operation of technology from the wider Internet, it can have connections with technology that exposes it to cyber risks in many ways, such as during software updates.

The threats are not limited to malicious attacks but can include unintended consequences resulting from the interconnectedness of onboard digital technology.

Class society Lloyd's Register has documented a situation in which updating software for a heating, ventilation and air-conditioning system on a mega-yacht resulted in air being sucked out of an engineroom, shutting down the engine and leading to a blackout.

Liberian Registry chief executive Scott Bergeron says shipping tends to lag behind technology adoption ashore, and therein lies the risk.

"As we come to grips more and more in our daily life in dealing with malware and viruses and things of that nature, it's time now for us to address these issues onboard these ships as they become more technologically sophisticated," he said.

Bergeron says the registry works with Bimco, ClassNK and the USMRC to identify the real threats to shipping and found that ships are vulnerable to the same risks as computer networks ashore: day-to-day practices can allow viruses and other maladies to proliferate.

And on ships, there are unexpected ways in which they can spread to operational systems.

"The net effect at this point that we've seen, doing some proper vulnerability testing, is that you will shut those systems down and create difficulties onboard," Bergeron said.

"Does it create a huge risk? Always, if some of your safety equipment doesn't work as you are expecting it to, it can create unanticipated risk."

The experts say that what shipowners have to do is not highly technical, but more a matter of policy and governance involving the practices of crews, as well as visitors to ships who access systems onboard. They recommend that shipowners carry out an assessment of their policies.

The US Coast Guard is aiming to update International Safety Management rules that will require shipowners to have cyber security management policies.

"Now they are going to be held accountable for this," Kline said. "You can't get away with the sticky note as a password any more."

TRENDING TODAY

1 Bulker newbuilding prices strengthen as enquiries roll in
Yards turn up the heat on some sizes as steel prices climb and good secondhand candidates evaporate

2 Marinakis pays over $150m for five ex-Hanjin boxships
Greek owner said to have outbid rivals for neo-panamax quintet

3 Collapse of 'Darling of Singapore' sparks fears banks will run away
Expected losses from Ezra bankruptcy could drive island's main lenders out of the offshore sector