Cyber crime is a recognized risk now to the shipping sector

AuthorDr. G. R . Balakrishnan

It is a regrettable fact that the convenience, productivity and efficiencies brought to everyone by modern connectivity and electronics, also bring with them a whole range of new vulnerabilities. Cyber crime, in all its various manifestations, is now a recognised risk and the shipping sector, like shore side industry, has to address this.

A first for the shipping industry, The Guidelines on Cyber Security Onboard Ships, was launched only last week and provides clear and comprehensive information on cyber security risks to ships. Developed by BIMCO and colleagues from CLIA, ICS, INTERCARGO and INTERTANKO, with expert support from a wide range of stakeholders, the guidelines will enable shipowners to take the right decisions to defend their vessels and organisations against attacks which could have serious consequences.

The guidelines identify the "enemy" represented by the activists, criminals, opportunists, terrorists and various state-sponsored elements who could mount a cyber attack on the industry, both afloat

and ashore. They provide an understanding of the nature of the potential threat and offers advice on how risks and vulnerabilities can be assessed, both in terms of individual companies, ships and third parties.

It demonstrates how these risks might be reduced, how practical contingency plans can be developed and a lot else besides in hardening the security of cyber systems afloat and ashore.

It is significant how these vulnerabilities have grown in recent years, with an ever greater dependence upon sophisticated electronic systems, computers, timing and the transmission of data. One might first think of bridge equipment like satellite navigation systems, AIS, and radar, but in terms of cargo management, propulsion and machinery controls, administration and communication systems, crew welfare and access control, these too are all to a greater or lesser degree vulnerable. The increasing dependence on data handling systems for everything from machinery maintenance to electronic documentation indicates the importance of this issue for the whole industry.

Various tests have demonstrated this vulnerability and shown how even quite primitive jamming equipment can cause real problems to those aboard a modern ship. Research has shown that it is technically possible to externally interfere with control equipment, while there have been incidents reported where ballast handling systems have been hacked into on an offshore craft and cargo data has been penetrated by criminals.

It is important that these vulnerabilities are properly understood and the guidelines point to the need for these issues to be high in the priorities of senior management, so that the right decisions are taken and adequate resources allocated. The guidelines have been written in clear and unambiguous language so that people who are not IT specialists are able to understand the issues that are explored. The

terminology is explained and the processes that need to be followed in hardening the defences are detailed in a practical fashion. Importantly, BIMCO and its partners in this important work recognise that this is a fast-changing scene and all will stay engaged so that where necessary, the information will be regularly updated. The guidelines are available to download from the website.

That cyber crime and threat is a veritable fact and not a science theory has been widely recognized by all those related to the shipping industry. The phenomenal development of technology, particularly Information Technology, has brought with it not only limitless advantages to humanity as a whole in terms of many industries that tend to enjoy and exploit speed and accuracy of details but also a highly sophisticated threat to the industries. Cyber criminals can hack the systems and steal away vital information so as to blackmail or damage the industry. The shipping sector cannot be an exception. As it is pointed out by a Captain, ships can be very high-value target for the cyber criminals.

Singapore Maritime Week 2016 relevantly concerned itself with the cyber crime and threat to the shipping industry.
"The maritime industry today is highly reliant on technology across virtually all fronts, from onshore to shipboard operations to navigation at sea. We believe it is time for the industry to now pay closer attention to this emerging risk. The inaugural Cyber Security Seminar at Singapore Maritime Week 2016 seeks to raise awareness of the need to be vigilant and to catalyse discussions on best practices to mitigate the risks posed by cyber security threats," said Maritime and Port Authority of Singapore (MPA) Chief Executive, Mr Andrew Tan.

Of course, it is not very difficult to foresee that soon the traditional Somali pirates would turn outdated, brushing aside less profitable but more risky way of piracy such as kidnapping and indulging in armed robbery and they will be replaced by highly intelligent and sophisticated anti-social cyber criminals who need not risk their lives sailing on the seas which are monitored by international navies but they would confine themselves to mere desktops, to say the least.

It is not only the shippers that are extremely worried about the cyber crime but also the insurers since they are inextricably linked with the industry. Insurers also are concerned with the shipping disaster that might result from a cyber incident. In its 2015 Safety and Shipping Review, Allianz Global Corporate & Specialty notes that "A cyber-attack could result in a total loss, leading to substantial insurance claims for hull, cargo and protection & indemnity underwriters. It could even involve multiple vessels from the same company."

Allianz says that the cost of a maritime disaster involving two megaships could reach $2 billion.

The enormously powerful internet becomes their weapon to attack the industry and the ships themselves. Their invasion is subtle and silent and the harm they inflict is massive.

The cyber security professionals talk about 'Advanced Persistent Threat'(APT). It is a network attack in which the hacker or the cyber criminal gains access to a computer network and stays there undetected for a very long period at times even of seven years. All that they do is to steal vital data rather than cause damage to the network. As a matter of course, these cyber criminals focus on very valuable information related to finance.

Cyber criminals can hack the port servers and sweep away lots of data pertaining cargoes, shipping routes which will effectively help pirates in their hijacking plans. Moreover, ports are more vulnerable, as Captain Rahul Khanna, Global Head of Marine Risk Consulting at Allianz observes, than ships which cannot be easily accessed through internet or a direct line. He said, "Their systems are not inter-connected like you would have in an average port."

The first step to fight this modern subtle evil is to know that it exists. The cyber security professionals say: 'Be proactive; be aware'. Going forward, it can be ascertained that ships as they are high-value assets will continue to attract the attention of the criminals who focus to benefit more since they take the risk. With LNG becoming increasingly shipped cargo, attacking the vessels for stealing LNG can be fairly expected.

With LNG being transported more and more, the thefts could prove very hazardous.

Captain Khanna said: "Theft is one of the big issues, you can have high value cargo stolen, or worst case scenario you can have sensitive cargo like weaponry or chemical cargos that can be used for terrorism.

"Although ships are less vulnerable and physical security measures are in place, if captured or hacked the damage to ships can be the most devastating."

Saying that statistics cannot be depended upon since many companies who get attacked do not generally report for fear of damage to their reputation, Captain Khanna urges that the use of white-hat hackers (specialist hackers who can pick up threats) can be put in place to pressure test the security systems to spot out the vulnerabilities in the system.

"Pressure testing of the system should pretty much be done by each and every port, and based on that contingency plans should be prepared by them for a breach if it takes place," Captain Khanna states, "I think some ports have done this but there are still places where this is being discussed and not implemented."

Endorsing what Captain Khanna says, the cyber security professionals also urge the stakeholders to have the network tested before it is

late. In fact, they even categorize the affected by the cyber crime into four types:

Those that have not been hacked and have an opportunity to protect themselves.
- Those that have been hacked and have done nothing.
- Those have been hacked and will be hacked again.
- Those that have been hacked and don't even know it (APT)

To put it simply, there are two major kinds of stakeholders: those who know they have been hacked and those who do not know yet. The problem with those who know that they have been attacked is that they would not reveal the fact for fear of damage to their reputation. This sort of concealment of facts in the long run fails to help fight the criminals. This is where what Captain Khanna says remains a relevant suggestion. He emphasizes creating a cyber security culture.

What is needed now is to create a cyber security culture within the industry that does not stop with just reporting the cyber attacks but makes it an international concern and standardizes security which can be implemented and held across ports and shipping so that despite advancements in criminal technology there is a common understanding and defence against the effects of cybercrime.

IMO and other maritime organizations have evidently been seized of the urgency of evolving international standards of cyber security systems.

It may be recalled here that February last, BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO together released a comprehensive guideline to tackle the cyber threat, The Guidelines on Cyber Security onboard Ships.