TECHNICAL CIRCULAR No. 470 of 06th March 2018

To:	All Surveyors/Auditors
Applicable to flag:	All Flags
	Cyber Security at Sea: The Real Threats
Reference:	CONARINA Class-Cyber Security

<u>Cyber Security at Sea: The Real Threats</u>

The maritime cyber security landscape is a confusing place. On the one hand, you have commercial providers suggesting the risks of everything from a hostile attack on ship's systems which allows the vessel to be remotely controlled by pirates and direct it to a port of their choice, or causing a catastrophic navigation errors, a phishing attack or ransomware on the Master's PC. While on the other, you have sensible people who point out that this notion is nonsense due to the number of fail safes and manual overrides and controls in place.

Then there are calmer voices still, who point out that the most likely threat is actually to the servers inside your head office, or a man in the middle attack on your company's bank accounts.

Recognizing the threats

So what are the real, documented, current threats to the shipping industry from cyber criminals?

Much has been made of the threat to vessels on the water from hackers. However, there is only limited available credible evidence to support claims of hacks at sea. Rather, the real threats on the water come from a lack of crew training and awareness and a culture which turns a blind eye to crew using their own devices at work and plugging them into ship systems to charge them, thereby possibly releasing a malware they may have been inadvertently carrying onto the vessel.

In 2017, I.H.S. Fairplay conducted a maritime cyber security survey, to which 284 people responded. 34 percent of them said that their company had experienced a cyber-attack in the previous 12 months. Of those attacks, the majority were ransomware and phishing incidents; exactly the same sort of incidents affecting companies everywhere, and not at all specific to the maritime world.

The good news is that only 30 percent of those responding to the survey had no appointed information security manager or department, meaning that the majority of companies have a resource able to respond and mitigate any attack.

However, the survey did reveal that there are still a lot of employees who have not received cyber awareness training of any kind, which means the shipping industry must try harder, for its own security.

Additionally, only 66 percent of those questioned said that their company had an IT security policy, which is a serious cause for concern; IT security cannot be approached on an ad hoc, incident by incident basis. It's the security equivalent of plugging holes in a hull with cardboard.

To underline that, 47 percent of those questioned believed that their organization's biggest cyber vulnerability was the staff. Hardly a glowing endorsement but, if you don't train your staff to be aware of threats, it's not surprising.

Mitigating the risk – train your staff

Imagine you're in charge of a company. You trust your staff to do everything. Except, it seems, ensure your bank accounts aren't handed over to cyber criminals or that your network is exposed to ransomware or malicious attack.

It would seem to be a rather curious way to run a company.

The key to mitigating cybercrime is training. A robust workplace IT security policy is the first step, but that can only work when also supported by a training course where employees can see the risks through demonstrations, simulations and good teaching.

There are very simple changes that any company can make to ensure better security in the workplace.

For staff dealing with accounts, additional rules may be required to ensure the risks of phishing and social engineering (whale attack) are reduced.

And similar attacks take place every week.

In the last six months, the shipping industry has seen several incidents in the sector, ranging from a data breach at Clarksons through to the damage done to Maersk by the WannaCry NotPetya variant sabotage/ransomware incident, which the company believes cost it as much as $300 million.

Regulatory compliance

The next major hurdle facing companies around the globe comes in the shape of the GDPR, which comes in to force in May 2018. It will affect companies in every sector, but the maritime industry in particular, given its global reach.

The new regulation introduces Privacy Impact Assessments (PIAs), which means that companies will be required to conducts PIAs wherever privacy breach risks are high in order to minimize risk to data subjects. Many companies may have to hire data protection officers in order to ensure compliance, while those companies dealing with EU crews will also want to take note of their liabilities in this regard.

The good news is that GDPR will also bring in common data breach protection notification requirements, so companies will be forced to report any breach of their systems within 72 hours, thus ensuring industry awareness and a better response time to potential vulnerabilities. This, in itself, may require staff training and is yet another aspect of GDPR companies need to be aware of.

Ultimately, the new regulations will be of benefit to everyone, but ensuring your company meets the right standards will be crucial. The days where maritime cyber security amounted to just making sure you turned the office PC off are long gone. Today, cyber security demands board room level attention as well as vigilance from all employees, be they in head office or out on the water.

REFERENCES:

- CONARINA Class – Cyber Security, David Rider

- ATTACHMENTS: No.

Kindest Regards,

Val Bozenovici
Naval Architect – Conarina Technical Director