Cyber Guidance for Crews

The Club thanks Steven Jones FRSA, specialist in maritime affairs, consultant and writer, for contributing this article.

The threats posed by maritime cyber security incidents are increasing, and the shipping industry is taking action to mitigate the risks while minimising the impact. The true extent of shipping's cyber vulnerabilities remains uncertain and the implications are growing, as is the concern of the effect of cyber security on the industry.

Every ship, whatever the size and trade, is potentially vulnerable and so seafarers need to know what is needed and expected of them to keep ships safe and secure. Understanding and awareness are key aspects of cyber security. All seafarers should be aware of not just the external threats, but of the problems they can introduce onboard too.

Connected ships

As shipboard systems become more sophisticated and connected, cyber security becomes ever more important. As vessel communication networks carry more data and faster, then this too has an effect and can make ships more vulnerable.

Hackers could theoretically target vessels and there is growing evidence that some may have done already. However, the bigger problem is actually what happens onboard.

Viruses and malware can have huge effects; they can render systems inoperable, or make them do the wrong thing. Whether that is propulsion systems, steering, fuel or navigation, everything is vulnerable.

Some 43% of seafarers in a recent survey said they had been on a vessel which had its systems affected by a virus. Many believed the viruses had been unwittingly introduced by the crew themselves. Seafarers are not routinely trained in cyber security 88% in the same survey claimed they were not aware of how to manage cyber issues onboard.

USB problems

Seafarers are in a difficult position; they can cause problems, but are unable to spot them. A major problem is the use of USB ports for charging mobile phones. According to one report, a seafarer recently plugged his smart phone into the ECDIS to charge it and as the phone began to update itself it wiped the entire chart folio.

New guidelines are emerging all the time, and it is vital that crews and managers ashore familiarise themselves with the issues, and that management systems or security procedures are based on best industry practice.

A key part of securing ships is making sure that all onboard embark on a simple 'cyber-hygiene' routine, making sure that any of the more obvious vulnerabilities are dealt with and addressed.

The basics

There are some absolute basics which vessels need to implement onboard as practicable actions that do not incur excessive overheads or complications:

- Set up strong user access control.
- Set up strong network access control.
- Perform back-ups.
- Test recovery plans.
- Make sure any anti-virus software is kept up-to-date.

Seeing cyber sense

Seafarers have very different roles onboard, and some have to deal directly with technology more than others. However, maritime cyber security can be threatened unwittingly and unknowingly if people are not operating with a view to their own cyber hygiene, and the actions taken by others onboard.

It is important to develop cyber sense:

Understand security basics: Learn what can go wrong and how, understand how to safeguard equipment and the vessel. Get a basic cyber security vocabulary.

Follow the Rules: Make sure any cyber rules are followed onboard.

Know the right tools & tactics: Know how to choose the right tools and actions to shield the vessel from viruses and malicious content.

Detection and prevention: Know how to identify cyber threats and how to respond.

Distrust Technology: Have some doubts and question what equipment is reporting. Do not blindly accept that technology is necessarily right.

Protecting those onboard and colleagues: Ensure that those onboard follow the correct procedures.

Safety Online: Protect online accounts (email, social media, cloud) and do not open files that haven't been checked.

Share with Care: Run virus checks on any files or removable drives that access shipboard computers.

Get real, useful cyber security skills: Think about how cyber attacks work, how to avoid virus infections and how these can be counteracted.

Be Aware: Accept that cyber issues are real and dangerous – do everything to prevent, protect and to react properly.

Shore to Ship: Ensure management ashore is working to support and educate those onboard.

Seafarers don't need to be an IT security expert to grasp the fundamentals of cyber risk, and the right measures can be introduced and applied fairly easily, by being sensible, aware and thinking about what can go wrong, then cyber security measures can be introduced at sea.