Superyacht Cybersecurity

Many of us look upon superyachts with awe as they glide through the waves with a bevy of beauties onboard, and with sleek lines of design which bring envy from their cousins in other parts of the Maritime industry. Over 5,890 superyachts are currently registered. Most are unique. All face similar provocations.

Superyachts are a microcosm of all the digital challenges that face seafarers.

Understanding what is needed on a superyacht to protect crew, guests and their owners from cyber-attacks is an excellent baseline for other seagoing vessels. We can all learn from superyacht experiences.

Cyber terrorists are very aware of seagoing vessels' vulnerabilities. Before the COVID-19 outbreak, the frequency of known attacks in the maritime sector had risen by more than 40% in just one year, according to a 2020 survey by BIMCO and Safety at Sea.

Since the start of the pandemic, maritime cyber-crime generally has increased by a much greater margin according to some estimates.

There is no reason to argue with experts who broadcast that superyachts have faced similar increases.

From 1 of January this year, cyber security came under the remit of the International Safety Management System (ISM) Code, supported by the IMO Resolution MSC.428(98), requiring shipowners and managers to assess cyber risk and implement relevant measures.

This is a comprehensive code, covering all eventualities- for all vessels.

How many superyacht owners have read it and how many crew members have implemented this advice?

Superyachts are a hybrid opportunity for cyber attackers. They have sophisticated information technology (IT) and operational technology (OT) built in.

Owners and guests bring their own IT vulnerabilities in the form of mobile phones, laptops, tablets and other digital devices. The risk is a rising curve as criminals see more opportunities for attack. Reputational damage is high on the list of outcomes together with

the results from unimpeded invasion of privacy and, of course, vessel and personnel safety.

A view from the front line

As one experienced crew member reported recently.

“I have been through five chief engineers on this yacht in the space of 13 months, all of whom have had different styles and ideas of how systems should work. The new chief had the bold idea to change the whole network onboard to make things simpler and easier for him to understand, much against our advice not to. We now have an arrangement whereby:

- There are printed IP addresses, usernames and passwords on every device from the Engine Control Room to the Bridge computing and AV racks.

- Remote access has been given to three different people in three different countries to try to solve some of the networking issues, one of which downloaded AnyDesk on our ECR computer so he could have remote access. I came down to the ECR the other day and someone was remotely connected to our main computer playing about with settings.

- Our email system was going to be changed from office365 with a secure random password to the open-source Mozilla Thunderbird with a generic password.

- Both internet firewalls installed have been causing problems with each other and subsequently they were both going to be removed before I stepped in.

- There is a proposal from the chief that our closed OT system PCs be upgraded to enable remote access to our new provider to save on the costs associated with flying out technicians.

No one is responsible for checking our cyber security at all.”

So, what should be done?

An approved IMO Maritime Readiness Assessment is a good place to start, but from a practical point of view, Owners and managers should work off guidelines which are verifiable, robust but simple and straightforward, enabling owners and managers to provide relevant information by questionnaire and buy in to feedback. From there, they can develop their own

risk-based strategy to provide a proactive and tailored approach which can then be developed in line with a rapidly diversifying range of risks to cover.

Insurance companies favour this approach. Owners and managers can no longer ignore the consequences. If there is no effective system in place, then insurance policies are invalidated but more importantly all on board are at risk.

Malcolm Warr is Chair of Maritime Services Management Ltd based in the United Kingdom