CYBERLOGIC

Clarity is confidence: **Navigating the murky waters of maritime cyber security**

With most modern businesses depending on technology and digital connectivity to operate, a breach, threat or upset in this area could leave any business dead in the water.

One of the most crucial business considerations is cyber risk management.

In technical terms, cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

Superyacht Cyber Security

While all industries are at risk of cyber-attacks, the superyacht industry has unique challenges that make implementing an innovative cyber security strategy particularly important. It goes without saying that a superyacht is a high-worth, moving asset that depends on sophisticated technology to operate the vessel. From the driving mechanics to the security cameras and multimedia on board, the technology interfaces are vital to operations. Additionally, superyacht clients are high net worth individuals who value connectivity, sensitivity and privacy.

The consequences of a cyber security breach are dangerous and can be devastating to the vessel and its clients. For the superyacht business, it is critically important that any cyber threats are proactively detected and managed. Shipping lines increasingly fear the hacking of onshore systems by perpetrators diverting hire or freight payments through elaborate phishing and spoofing tactics and, as a result, the shipping lines have procured appropriate business liability cover. That said, cover comes hand-in-hand with strict compliance.

In a world where cyber threats are on the rise the new IMO (International Maritime Safety Organization) resolution (MSC.428(98), mandatory for ships as of 1 January 2021, is designed to support safe and secure shipping. The IMO is not prescriptive in how these safety recommendations should be implemented – clients are free to choose whatever path is best suited for their environment.

Cyberlogic Solutions

Cyberlogic’s recommended approach to cyber risk management is not a once off exercise, but rather something that needs to be looked after. The key is to ensure an ongoing balance between onboard flexibility and an effective security posture, with minimal noticeable disruptions. Our Vulnerability Managed Services offer a closely monitored security service amplified by our state-of-the-art tooling that uses AI technology to identify, protect, detect and respond to any threats based on predefined policies. When a threat is detected our Security Operations Centre (SOC) is ready to validate the risk and either block or endorse the event.

Cyberlogic’s hand-picked team is made up of highly-niched technical experts in all areas of cyber security. Through extensive work and customised experience with superyachts, the Cyberlogic team is skilled in handling the specific difficulties that come with securing these vessels’ systems.

In 2018, Cyberlogic was employed to carry out a cyber security system assessment and vulnerability analysis for a fleet of superyachts. This initial exercise marked the start of a rewarding project and Cyberlogic has since worked with the entire fleet to ensure their systems are expertly protected, monitored and updated.

So what exactly did it involve?

Comprehensive Assessment

Completion of an initial Onboard Cyber Assessment Questionnaire by the ETO and AV/IT partners in conjunction with Cyberlogic. This questionnaire has 18 sections and covers areas such as policies, access control, connectivity, backups, firewalls and more.

Bespoke Strategy

A report drafted with findings from both the Questionnaire and the Vulnerability Assessment detailed remediation actions to ensure increased security of all on board. This report enabled a clear strategy for cyber security for the whole fleet, with bespoke security solutions that spoke to the unique needs of each vessel.

Implementation

Focussing on long-term success of cyber security, the Cyberlogic crew worked collaboratively with the IT teams on board to implement the remediation actions. The collaboration included training and access to relevant systems to further bolster the proactive protection of the fleet's systems. In order to better comply with IMO regulations, Cyberlogic also provided best easily implemented practice policies as well as staff training in accordance with Standard Operating Procedures (SOPs).

Fleet Captain and Director of Maritime Operations, sums up his experience with Cyberlogic:

“Engaging the expert team of professionals at Cyberlogic to assess and consult on our cybersecurity threats and protection options has been **a huge success from the outset.** They quickly established our security weaknesses via a vulnerability test and audit, and produced a thorough , bespoke report that explained the results in clear language. After implementing control measures, **we now have strengthened our systems against serious threats** and they are proactively monitored 24/7, **giving us great peace of mind.** What started as a potential headache, now feels like an **expertly managed project.** Cyberlogic has integrated with our AV/IT partners and the onboard team seamlessly; **it’s a great partnership.**”

Let our team help you secure your systems - maritime or other.

While cyber attacks themselves are malicious actions which can cause lost revenue, lost or exposed confidential information, blackmail or a loss or delay in a company's activities, the effort to mitigate these attacks and comply with MSC laws does not need to be intimidating or difficult.

At Cyberlogic we work collaboratively with clients to build and manage the most appropriate technology solutions.

Book an initial risk audit with Cyberlogic's cybersecurity experts today.

+27 861 111 202

HELLO@CYBERLOGIC.CO.ZA