Why should I train my crew and shoreside staff to be aware of the cyber risks, threats and vulnerabilities to yachting?

PEOPLE ARE THE GREATEST RISK

People are now proven to be the greatest cybersecurity risk with employee error or negligence being the single most significant cause of both cyber and data breaches. Statistics across the globe continue to show that employees cause around 90% of all cyber and data breaches suffered by businesses.

Therefore, deploying technical responses such as firewalls, intrusion prevention systems, antivirus software, spam filters etc. is no longer enough. As such, for the past several years, the concerns around the cyber risks caused by crew and shoreside staff has become a major issue highlighted by many industry cybersecurity guidelines and maritime trade bodies alike.

ISM CODE REQUIREMENTS

Recognising the urgent need to raise awareness of cyber risks, threats and vulnerabilities, in June 2017, the IMO adopted Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems. Now formally part of the ISM code, cyber risk management is to become an integrated part of onboard safety and security that must be addressed no later than January 2021.

The ISM code guidelines state that effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organisation. Further guidance states that an adequate ongoing training and awareness program is a crucial element of onboard and shoreside cyber risk management.

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR imposes a legal requirement on almost every EU business to ensure personal data is securely protected against such issues as unauthorised or unlawful access and use, accidental loss, destruction or damage. GDPR requires businesses to use appropriate technical or organisational measures to protect personal data. Again, in response to the overwhelming evidence that people are the greatest risk to cyber and data breaches, adequate training and awareness is a vital organisational measure.

ACT NOW

Regardless of the size of the vessel, the number of crew, the need for mandatory industry compliance or legal requirement, adequate cybersecurity is not only a vital feature in minimising cyber risk and liability but more importantly in ensuring onboard safety and security of passengers, guests and crew alike.

THE COURSE – MARITIME CYBER RISK AWARENESS TRAINING

In direct contrast and equally the greatest opportunity to minimising cyber risk is to empower and train crew and shoreside staff with an awareness and understanding of the cybersecurity issues and challenges they are faced with in their every-day onboard and shoreside activities.

Designed and developed specifically for yacht crew and shoreside staff by Dr Paul Hunton, a leading cybersecurity expert with MCS, the course content has been quality assured and accredited in the UK by the world-leading cybersecurity agency GCHQ.

The course content and syllabus have taken the maritime industry best practice guidelines, the imposed requirements of the ISM code and the legal implications of GDPR to ensure crew and shoreside staff are both prepared and aware of the cyber risks, threats and vulnerabilities that face yachting.