



Fully Online
**Cyber Security Awareness
for Superyacht Crew & Staff**



About the Course

An awareness of cyber security-related threats amongst the crew and staff of Superyachts is generally quite poor. This can lead to breaches of security, and open the yacht, personnel, guests and owners to potential cyber security attacks, as well as stealing and misuse of personal data.

By providing the crew and staff with an awareness of these threats, especially those connected with social media hacking and ID theft, this will lead to increased security for the company, yacht and personnel involved.

The 'Cyber Security Awareness for Superyacht Crew & Staff' course provides an overview of the cyber threats that exist, risk management, and cyber security compliance for Superyachts.

The course also looks at issues for crew & staff with social media, then examines the measures that can be taken to mitigate and defend against these types of threats. This course is designed to provide the user an awareness of Maritime Cyber Security issues because 'cyber security is everyone's responsibility.'

Course Duration

The course lasts for approximately 1.5 hours depending on the learner's abilities and reading speed. However, you can enter and exit this course as often as you require.

Target Audience

This course is aimed at all crew and staff personnel of Superyachts, Motor Yachts & Mega Yachts who access personal social media, websites, and other vulnerable applications through shipboard and personal devices such as smartphones, tablets, laptops and desktops.

The course is also ideal for guests and owners to appreciate the risks involved, and how to assist in the mitigation of those risks through personal cyber security measures whilst on board the yacht.

Regulations Addressed

The course has been designed to provide an overall awareness of the Cyber Security requirements for Superyacht crew and staff at all levels in line with IMO 2021 and MSC.428(98).

Awarding Body

Learners will receive a Certificate of Completion upon completion of this online course through VIRSEC Ltd.



Course Subjects

The following are the main subject heading for the course. There are many sub-headed areas contained within this course covering an impressive amount of content relevant to the crew & staff.

- Course Introduction Area
- Cyber Risk Management
- The Foundation for IMO 2021
- MSC.428(98) Cyber Security Compliance for Superyachts
- Compliance Requirements for IMO 2021
- Crew Training & Awareness Requirements
- Maintaining a Safe & Secure Social Media Environment
- Geographical Security for High-Value Assets with a Focus on Cyber Security

Why Take This Course

- ✓ The course is relevant to the crew and staff who work on yachts
- ✓ The course follows advice provided in MSC.44288(98) and IMO 2021
- ✓ Subjects covered encourage crew and staff to consider the threats associated with personal social media accounts, ID theft, misuse of data, etc.
- ✓ Decrease the vulnerability of the Yacht to acts of Cyber-related security issues for crew, staff, owners and guests
- ✓ The course is fully online, accessible via a reliable internet connection, or available as an offline course via a downloadable App.
- ✓ Full set of course notes available as a secure PDF download for use as revision material
- ✓ Follows a detailed course outline developed by industry experts
- ✓ Focuses on the prevention of cyber security-related incidents and mitigation strategy

Course Pricing

This online course is £45 UK Pounds [+VAT] per person or the equivalent of an associated currency at the time of purchasing this course. Email us to learn about bulk course booking discounts.

Discount Offer

If you purchase this course today, please use the following coupon code to receive **10% OFF** the listed course price.

MAR-SEC-10



+44 (0)161 763 4427



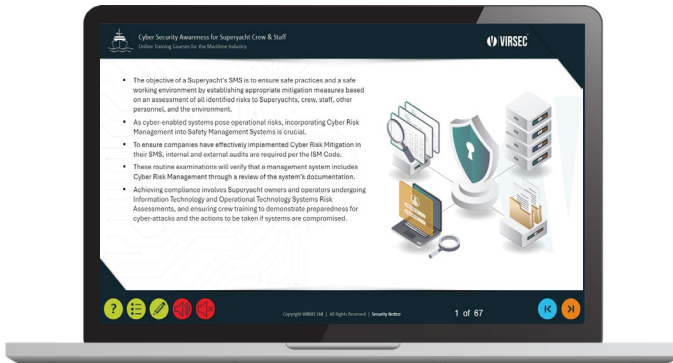
www.virsec.org



training@virsec.org



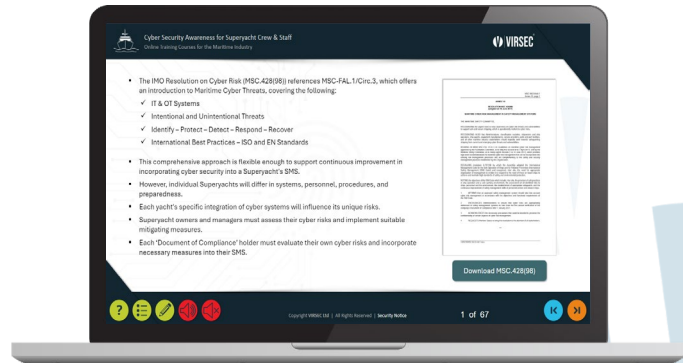
Sample Course Slides



Cyber Security Awareness for Superyacht Crew & Staff
Cyber Training Course for the Maritime Industry

- The objective of a Superyacht's SMS is to ensure safe practices and a safe working environment by establishing appropriate mitigation measures based on an assessment of all identified risks to Superyachts, crew, staff, other personnel, and the environment.
- As cyber-enabled systems pose operational risks, incorporating Cyber Risk Management into Safety Management Systems is crucial.
- To ensure companies have effectively implemented Cyber Risk Mitigation in their SMS, internal and external audits are required per the ISM Code.
- These routine examinations will verify that a management system includes Cyber Risk Management through a review of the system's documentation.
- Achieving compliance involves Superyacht owners and operators undergoing Information Technology and Operational Technology Systems Risk Assessments, and ensuring crew training to demonstrate preparedness for cyber-attacks and the actions to be taken if systems are compromised.

Copyright VIRSEC Ltd | All Rights Reserved | Security Notice 1 of 67



Cyber Security Awareness for Superyacht Crew & Staff
Cyber Training Course for the Maritime Industry

- The IMO Resolution on Cyber Risk (MSC.428(98)) references MSC-FAL.1/Circ.3, which offers an introduction to Maritime Cyber Threats, covering the following:
 - IT & OT Systems
 - International and Unintentional Threats
 - Identify - Protect - Detect - Respond - Recover
 - International Best Practices - ISO and EN Standards
- This comprehensive approach is flexible enough to support continuous improvement in incorporating cyber security into a Superyacht's SMS.
- However, individual Superyachts will differ in systems, personnel, procedures, and preparedness.
- Each yacht's specific integration of cyber systems will influence its unique risks.
- Superyacht owners and managers must assess their cyber risks and implement suitable mitigating measures.
- Each 'Document of Compliance' holder must evaluate their own cyber risks and incorporate necessary measures into their SMS.

Download MSC.428(98)

Copyright VIRSEC Ltd | All Rights Reserved | Security Notice 1 of 67



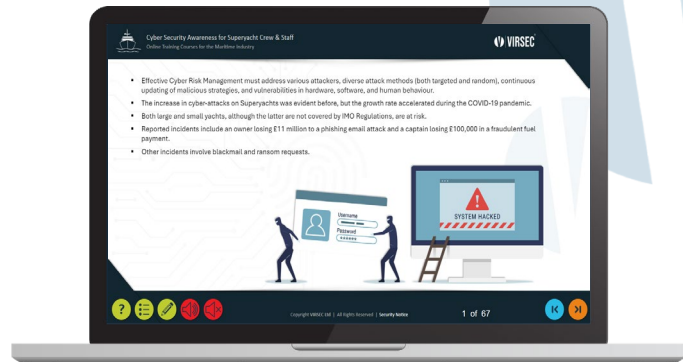
Cyber Security Awareness for Superyacht Crew & Staff
Cyber Training Course for the Maritime Industry

- Integrating cyber risk into the SMS can take several months, depending on the complexity of the onboard systems.
- Inspections require a combination of technical mitigations, revised procedures, and crew training to develop a practical and cost-effective route to compliance.
- The ISM Code advises that new risks be accommodated as soon as possible, making the SMS a 'live' document that is regularly updated and improved as risks evolve.

ISO 27001 INFORMATION SECURITY INTERNATIONAL STANDARD

ISM Code

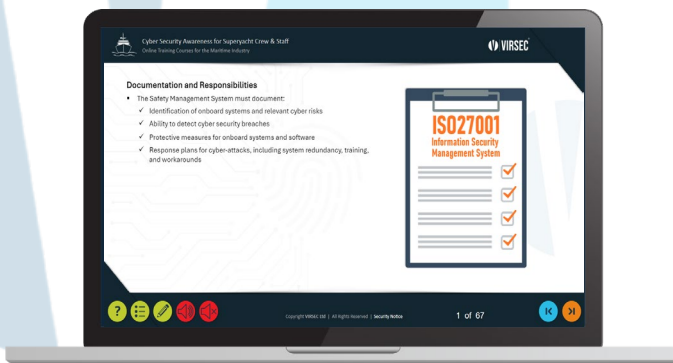
Copyright VIRSEC Ltd | All Rights Reserved | Security Notice 1 of 67



Cyber Security Awareness for Superyacht Crew & Staff
Cyber Training Course for the Maritime Industry

- Effective Cyber Risk Management must address various attackers, diverse attack methods (both targeted and random), continuous updating of malicious strategies, and vulnerabilities in hardware, software, and human behaviour.
- The increase in cyber-attacks on Superyachts was evident before, but the growth rate accelerated during the COVID-19 pandemic.
- Both large and small yachts, although the latter are not covered by IMO Regulations, are at risk.
- Reported incidents include an owner losing £11 million to a phishing email attack and a captain losing £100,000 in a fraudulent fuel payment.
- Other incidents involve blackmail and ransom requests.

Copyright VIRSEC Ltd | All Rights Reserved | Security Notice 1 of 67



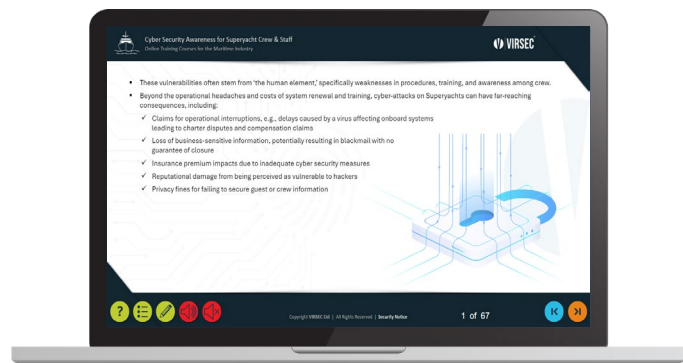
Cyber Security Awareness for Superyacht Crew & Staff
Cyber Training Course for the Maritime Industry

Documentation and Responsibilities

- The Safety Management System must document:
 - Identification of onboard systems and relevant cyber risks
 - Ability to detect cyber security breaches
 - Protective measures for onboard systems and software
 - Response plans for cyber-attacks, including system redundancy, training, and workarounds

ISO 27001 Information Security Management System

Copyright VIRSEC Ltd | All Rights Reserved | Security Notice 1 of 67



Cyber Security Awareness for Superyacht Crew & Staff
Cyber Training Course for the Maritime Industry

- These vulnerabilities often stem from 'the human element', specifically weaknesses in procedures, training, and awareness among crew.
- Beyond the operational headaches and costs of system renewal and training, cyber-attacks on Superyachts can have far-reaching consequences, including:
 - Claims for operational interruptions, e.g., delays caused by a virus affecting onboard systems leading to charter disputes and compensation claims
 - Loss of business-sensitive information, potentially resulting in blackmail with no gain-free of closure
 - Insurance premium impacts due to inadequate cyber security measures
 - Reputational damage from being perceived as vulnerable to hackers
 - Privacy fines for failing to secure guest or crew information

Copyright VIRSEC Ltd | All Rights Reserved | Security Notice 1 of 67



Contact Us

VIRSEC Ltd.
Units 2a(i) & 2a(ii)
Beehive Mill
Jersey Street
Manchester
M4 6JG
United Kingdom

T: +44 (0)161 763 4427

E: training@virsec.org

W: www.virsec.org