Cyber Security at Sea Training Course

Overview

The shipping industry has recently been alerted to the impact that cyber threats have had on businesses of all sizes around the world. These very real threats have come in the form of high-profile ransomware and other computer system breaches, that could severely affect the safety of any company's crew, not to mention its reputation.

Ships' systems and operations are becoming increasingly networked, making them more vulnerable to cyber breaches. Once malware gains access to one part of a vessel's IT system, there is a chance it may impact heavily on other areas of the ship too.

This course raises awareness of cyber security onboard ship and encourages good cyber 'hygiene'. It explores cyber security risk and introduces candidates to the cyber risk management plan.

Course Delivery and Assessment

This standard level KVH Videotel course comprises an introduction, video (28 minutes, with optional subtitles in English or simplified Chinese), reference workbook, tutorial and course test.

This course:

- Explains what the risks are, where they come from, and their consequences for the individual, the ship and the company
- Outlines the shore office’s responsibilities for protecting the ship's systems
- Suggests how the Master can assess the ship's vulnerabilities
- Shows how to reduce the risks on ships by following correct procedures and applying effective cyber 'hygiene'
- Provides guidance on the steps to take when shipboard personnel become aware of a cyber security threat

Regulations Addressed

KVH Videotel’s Cyber Security at Sea Training Course has been developed in accordance with:

- MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management

This course will assist in the provision of cyber security awareness training as noted in programmes such as TMSA3, VIQ7 etc.
By the end of this course, candidates should be able to understand:

- Cyber security threats – where they come from, that they are, what consequences they can have for the ship, individuals and the company

- That the International Maritime Organization (IMO) now requires companies to include a cyber risk management plan in the Safety Management System (SMS)

- How to assess the risks to the ship’s IT (information technology) and OT (operational technology).

- How the risks can be reduced

- How to respond to a cyber security breach or attach

- The fact that the threats will inevitably evolve in future, necessitating constant vigilance and reviews of the cyber risk management plan

### Cyber Security at Sea Training Course

<table>
<thead>
<tr>
<th>Standard Level Course</th>
<th>Guided learning hours</th>
<th>Video and reference workbook delivered as computer based training (CBT)</th>
<th>Tutorial (self-test)</th>
<th>Final onscreen multiple-choice assessment (Pass mark 70%)</th>
<th>Time to complete the course</th>
<th>Course fee</th>
<th>Certification fee</th>
<th>Discount available for multiple enrolments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>2-3</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Up to 90 days</td>
<td>Price Band A</td>
<td>Included</td>
<td>Price Band A</td>
</tr>
<tr>
<td>Via company subscription (e.g. VOD, VPM etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td>Included</td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Certification

All candidates for the issue of a certificate by KVH Videotel, must complete a Course Enrolment and Certification Application Form and be directly supervised completing their final onscreen assessment by an authenticating person. Authenticating persons include the Master or Chief Engineer onboard ship or senior representative of a registered shipping company or maritime institution onshore. KVH Videotel’s standard level course procedures list the documents to be sent to us on completion of the Cyber Security at Sea raining course.

Please refer to the following documents for further information:

- ‘Course Enrolment & Certificate Application Form’ - FORM F1
- ‘Course Overview’ sheet - INF 01
- ‘Electronic Submission of Documents’ sheet - INF 02