informa
corporate learning

ISM 2021. CYBER SECURITY RISK MANAGEMENT

CAPTAIN MICHAEL QUAIN

Independent
Marine Consultant
Quain Marine Services

A few years ago I arrived on board an Aframax tanker to carry out a routine annual internal audit of the vessel's Safety Management System as required by the ISM Code. I went on to the bridge to find the master at the bridge communications system computer looking rather stressed. He had spent the past hour on the phone with a member of the IT department trying to find a fault with the on-board computer network. The system was riddled with viruses. The company SMS, which was entirely computer based, could not be properly opened. The master's stress was compounded by the IT person who was not able to allow for the fact that the master was not an IT expert and had no idea what he was being told to do.

More recently I attended a VLCC, which was on a bareboat charter, on behalf of the head owners. They instructed me to check that the ship was being properly cared for by the charterers and their designated technical managers. I arrived on the bridge to find the master in consultation with another man who turned out to be a member of the manager's IT department. He had just completed cleaning the ship's computer system which had been infected with viruses. That company also had a fully electronic SMS.

ISM Code section 11 requires that "the company should establish and maintain procedures to control all documents and data which are relevant to the safety management system" and further that "valid documents are available at all relevant locations". If the computer-based SMS is infected such that documents cannot be controlled or made available then a major non-conformity would apply rendering the vessel's Safety Management Certificate invalid. The ship is not seaworthy.

Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitisation, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

This is not a new phenomenon, that first ship audit I just described was 6 years ago. So it is somewhat surprising the IMO has only recently decided to take action.

In June 2017 IMO published a one-page circular letter MSC.428(98) "Maritime Cyber Risk Management in Safety Management Systems". Paragraph 2 of this letter "Encourages Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021".

As we approach the deadline I have spoken to many senior staff of ship managers who seem bewildered about the "huge technical challenge" of establishing a cyber risk management system. It is certainly of huge importance, but it is not a huge task nor is it entirely technical. The first line of protection in any risk and safety management process is the human element. Education, training and enforcement of documented procedures must be our staring point.

Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organisation and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

Effective Cyber Risk Management consists of five functional elements:

- **Identify** - Define personnel roles/responsibilities for CRM and identify systems, assets, data and capabilities that, when disrupted, pose risks to ship operations
- **Protect** – Implement risk control processes and measures, and contingency planning to protect against a cyber event and ensure continuity of ship operations
- **Detect** – Develop and implement activities necessary to detect a cyber event in a timely manner
- **Respond** – Develop and implement activities and plans to provide resilience and restore systems necessary for shipping operations or services impaired due to a cyber event
- **Recover** – Identify measures to back up and restore cyber systems necessary for shipping operations impacted by a cyber event

These five elements could be applied to any type of Risk Management Strategy.

ABOUT THE AUTHOR

Captain Michael Quain has 50+ years service in the maritime industry most of it in or around the management of tankers. During 28 years at sea he served on dry cargo ships and tankers including 11 years as master on oil and chemical tankers. After moving ashore, he worked as operations manager for a tanker owner, as a marine superintendent and then manager of the marine department of a ship management company in Limassol. For 15 years he was an OCIMF SIRE inspector accredited for inspecting oil, chemical and gas tankers with over 600 SIRE inspections completed. He also carried out over 30 assessments of Tanker Operator's management systems on behalf of oil major clients with reference to the OCIMF TMSA system.

He is a lead auditor under the ISM Code as well as ISO Management Standards and offers consultancy services to clients legal teams as an expert witness in litigation and arbitration cases involving tankers.

Since 2015 he has been an Academic Course Director with Lloyds Maritime Academy responsible for a one-year on-line distance learning course in Tanker Management for which he personally wrote all study modules as well as set and mark all student assignments and examinations.

Michael is a Younger Brother of Trinity House, a Fellow of the Nautical Institute, a Freeman of the Honourable Company of Master Mariners and is a member of the Royal Institute of Navigation.

ONLINE TRAINING: TANKER MANAGEMENT

6 modules I 1 hour per week I 2nd August - 10th September 2021

In an increasingly technical and regulatory environment the oil, gas and petrochemicals shipping sector encompasses some unique challenges.

Tanker Management is a professional development course that develops a thorough and detailed knowledge and understanding of the design, technical, operations, legal and managerial challenges that need to be addressed for an individual or company to be successful in the management of all tanker types.

From the types and design of vessels used to the way the cargo is handled, from understanding the inspections undertaken to how a vessel is chartered by the oil and gas majors, from onboard operations to terminal management, and from the ship/shore interface to commercial operations and management, every aspect of business is examined in detail.

For more information, contact us on **+65 6973 3567** or email **sgtraining@informa.com**.