FAIRMONT SHIPPING SINGAPORE
TAMAR SHIP MANAGEMENT

CYBER ATTACK – OPERATIONAL TECHNOLOGY (OT) SYSTEM MALFUNCTION / COMPROMISE

43

	ACTION (NOT NECESSARILY IN ORDER)
☐	Treat failure of OT systems due to a cyber incident like any other equipment failure e.g. activate ECDIS failure contingency in case of cyber attack on ECDIS; activate power failure contingency in case of cyber attack on A/Es power management; if VFD is corrupted, switch the system off and run the Engine Room as a traditional Engine Room; switch over to manual system in case of failure of an auto control system etc.
☐	Remove the cyber threat by isolating the compromised OT System from rest of the IT infrastructure, disconnect the interface with rest of the equipment/ disconnect the LAN cable e.g. in case of an ECDIS is compromised, isolate it with 2nd ECDIS.
☐	Portable media used on this equipment to be quarantined until further instructions received from the Office. Stop any identified practices that led to the data breach.
☐	Concerned staff on board are to be made aware of the equipment failure.
☐	Take action to ensure the immediate safety of the crew, ship, cargo and protection of the marine environment. Assess the impact on the safe operation of the ship.
☐	Check whether failure is due to Is any shore-based person currently completing any software modifications either remotely or whilst onboard the vessel.
☐	CALL THE OFFICE IT DEPARTMENT ON THE FOLLOWING: IT Emergency Response (24 H) Tele: +27 (0)79 902 5219 Please also inform your Ship Manager
☐	The duty IT representative and Ship Manager will guide the Master through the process of confirming the extent of the breach of the Cyber security on the Vessel's OT infrastructure.
☐	Send the details of the OT system failure to office – this may include screenshot of the display/error message/test result/alarm indication etc.
☐	IT response team to consult Cyber Security Consultants to advise the Emergency Response Team on the procedure to follow in addressing and recovering from a Cyber Security attack as applicable.
☐	Office to notify the cyber attack on OT system to concerned parties
☐	Carry out the initial assessment: • how the incident occurred • which IT and/or OT systems were affected and how • the extent to which the commercial and/or operational data is affected • to what extent any threat to IT and OT remains.
	Activate the recovery procedure using remote help from the respective service provider, general recovery procedure is as follows: • Remove the threat • Clean up the programme • If clean-up is not possible, restore the programme from a backup (if backup • available on board) or • Attendance on board by an authorized service provider or • Purchase new OT System/equipment if necessary