Cyber-attack on vessel

Safety Flash Published on **5 November 2026** Generated on **5 November 2026** IMCA SF 19/26

What happened?

An oil tanker operated by one of our Members suffered a cybersecurity incident in which the operating systems and stored data on multiple work PCs connected to vessel's onboard server, were deleted, and the ship's external email communication and vessel management programs were disrupted. The incident occurred on a passage from Egypt to Galveston, Texas.



The vessel was subsequently boarded by the American Coastguard and the FBI, with consequent additional delay and negative publicity.

The detailed learnings from the incident may form part of other IMCA publications.

What was the cause?

The nature of the damage was consistent with Wiper-type attacks, which focus on system destruction rather than financial demands. Following the incident, the attacker sent mocking emails containing political and ideological statements and claiming to have seized control of the vessel. The vessel and the company convened their emergency response teams, isolated PCs and servers suspected of being infected from the network, and changed the public IP address and the business network's IP range. They restored the vessel's operating system and data on the server as well as the email service, recovered a backup, and formatted and reinstalled the infected PCs. No abnormalities were found during inspections of key OT systems; therefore, the actual damage was assessed to be limited to the IT business network.

However, at the time of the incident, there were no additional security devices directly managed by the company beyond the telecom provider's firewall; long-term log retention was limited; and a licensing structure that made it difficult to update the firewall firmware was identified. Furthermore, the fact that destructive activities spread to PCs connected via the LAN after the server or accounts were compromised suggests that the internal barriers within the business network—including segmentation, access control, behaviour-based detection, and privilege management—may not have been sufficient.

At this stage, the initial point of entry has not been confirmed. However, it was reported that the affected vessel lacked a sufficiently up-to-date communications and security environment; the existing VSAT environment allowed for public IP addresses or external remote access; and there were deficiencies in the telecom provider's firewall policies, long-term log retention, firmware updates, and the

company’s managed secondary firewall. The preliminary root cause is a combination of structural vulnerabilities: an outdated and poorly maintained communications security environment, reliance on a single perimeter defence, a lack of internal network segmentation, and insufficient centralized detection, logging, and recovery controls—rather than the type of communication line itself.

Lessons learned

- A cyber incident affecting business IT can create serious operational and potential marine-safety consequences even when no OT-system damage is identified.
- Rapid network isolation is essential, but containment should be coordinated with forensic evidence preservation.
- Sufficient firewall, server, endpoint and remote-access logs are necessary to determine the intrusion route and support an effective investigation.
- Cybersecurity should not rely solely on a telecommunications provider’s firewall. Additional independent control, visibility and assurance should be in place.
- The type of satellite communication service is not the determining security factor. VSAT, Starlink and other services should be protected by the same company-controlled security architecture.
- Central servers and interconnected business networks require segregation, restricted privileges, endpoint monitoring and resilient backups to limit the potential impact of compromise.
- Temporary actions such as changing public IP addresses or blocking email domains should be followed by vulnerability removal, forensic verification and effectiveness testing.

IMCA Safety Flashes summarise key safety matters and incidents, allowing lessons to be more easily learnt for the benefit of the entire offshore industry.

The effectiveness of the IMCA Safety Flash system depends on the industry sharing information and so avoiding repeat incidents. Incidents are classified according to IOGP's Life Saving Rules.

All information is anonymised or sanitised, as appropriate, and warnings for graphic content included where possible.

IMCA makes every effort to ensure both the accuracy and reliability of the information shared, but is not be liable for any guidance and/or recommendation and/or statement herein contained.

The information contained in this document does not fulfil or replace any individual's or Member's legal, regulatory or other duties or obligations in respect of their operations. Individuals and Members remain solely responsible for the safe, lawful and proper conduct of their operations.

Share your safety incidents with IMCA online. Sign-up to receive Safety Flashes straight to your email.