Maritime Cyber Security Stats and Facts

FACTS

Scenarios Where Injuries Can Occur Due to Maritime Cyber Incidents

1. A ship’s navigation system is compromised through a cyberattack and leads to incorrect or manipulated navigational data resulting in collisions with other vessels, grounding, or incidents involving maritime infrastructure like bridges or offshore structures.
2. Cyberattacks targeting a ship’s engine or machinery systems can cause engine failures, propulsion system malfunctions, or loss of power can lead to accidents and injuries.
3. Cyber incidents that disrupt communication systems, including ship-to-ship, ship-to-shore, or emergency communication channels, can hinder effective coordination and response during critical situations.
4. If maritime vessels’ safety systems, such as fire suppression, alarm systems, and emergency response mechanisms, are compromised through cyberattacks, it impairs functionality, potentially leading to delayed or inadequate responses to safety incidents and increasing the risk of injuries.
5. Cyber incidents targeting access control systems, such as electronic locks, security cameras, or entry control mechanisms, result in unauthorized access to sensitive areas of a vessel or maritime facility.

STATS

- Three-quarters of maritime professionals believe a cyber incident is likely to force the closure of a strategic waterway (76%). More than half expect cyber-attacks to cause ship collisions (60%), groundings (68%), and even result in

physical injury or death (56%) as an overwhelming majority (79%) of professionals say the industry considers cyber security risks to be as important as health and safety risks.

    - According to the survey, barely 3 in 10 (31%) maritime professionals believe that organizations within their sector are effective at sharing information and lessons learned about cyber security risks, threats, and incidents.

- On the cyber security front, 2021 was not a good year for the maritime and logistics industry. Attacks targeting ships increased in frequency by 33 percent – and that came on the heels of a 900-percent increase in attacks against ships and port systems in 2020.
- In a 2020 Safety at Sea and BIMCO Maritime Cyber Security survey, despite the majority of respondents (77%) viewing cyber-attacks as a high or medium risk to their organizations, few appear to be prepared for the aftermath of such an attack. 64% of respondents said their organization has a business continuity plan in place to follow in the event of a cyber incident, but only 24% claimed it was tested every three months, and only 15% said that it was tested every six to 12 months. Only 42% of respondents said that their organization protects vessels from operational technology (OT) cyber threats.