beazley

Article

Cyber risk at sea: Why lenders are changing course

What happens when a vessel goes dark mid-ocean; not from a storm, but from a cyberattack?

The fallout can be disastrous, and until now, lenders had limited safeguards against this invisible threat. That era may just be over. The risks are now systemic and can ground a vessel or derail a supply chain.

For the first time, BankServe (a leading global broker) urged lenders to make cyber protection a condition of lending. This was explicitly laid out in a circular by the business, and means that if/when lenders follow suit, what was once optional is now essential.

Yesterday’s protections were enough – until they weren’t

For years, lenders relied on Hull and Machinery and War Risk insurance to safeguard maritime assets and a pre-requisite for mortgages. With the growing Cyber threat, that calculus has changed – the threat is now pressing. This is the result of several different drivers:

- **Regulatory pressure:** Europe’s NIS2 directive and new U.S. Coast Guard rules have rolled out tighter controls around cyber resilience and incident reporting across shipping and the wider maritime industry. Falling short risks, penalties, operational restrictions, market barriers and reputational harm.
- **Significant incidents:** A recent Iranian cyberattack disabled navigation systems on more than 60 vessels, likely forcing costly repairs and operational downtime. Every hour offline disrupts operations, adds financial exposure and risks physical damage.
- **Escalating risks:** Increasingly common spoofing and jamming attacks use false or blocked GPS signals to mislead or disable a vessel’s navigation systems. They can trigger groundings, collisions,

or border violations, escalating routine journeys into costly operational endeavours.

- **Market ambiguity:** Traditional Hull and Machinery policies often include cyber exclusions, creating uncertainty about coverage for incidents like GPS spoofing, jamming and software-as-a-service (SAAS) provider failures.

What this shift means for key stakeholders

At a time of increasing geopolitical uncertainty, cyber coverage is no longer a technical adjustment, clarity of cover is a strategic imperative. Here's how the new reality reshapes responsibilities across the maritime ecosystem:

- **Lenders: Cyber becomes due diligence**
  Cyber insurance is becoming a consideration of lenders and may become a condition to protecting financed assets against emerging digital threats, and shield lenders from cascading financial risk.
- **Shipowners: Coverage and compliance**
  Operators must adopt robust cyber policies and strengthen onboard protocols to prevent and respond to attacks. The cost of inaction? Operational downtime, reputational damage, potential loss of financing and regulatory penalties.
- **Insurers: Rethinking policy language**
  Traditional frameworks won't cut it. Policy wording, pricing models, and buy-back clauses need to evolve to address digital risks alongside physical ones. The market is demanding clarity – and flexibility.

From a technical glitch to a systemic risk

BankServe's advisory reframes the conversation. It moves the industry from reactive to proactive, urging stakeholders to confront the realities of cyber risk to strengthen maritime resilience.

The message is clear: ignore cyber risk, and you jeopardise your capital. Now it's no longer about whether cyber risk matters – it's how the industry will respond.

Discover Beazley's **Cyber Defence for Marine**.

Beazley's Cyber Defence for Marine gives shipowners and lenders the clarity and protection they need as cyber insurance becomes a strategic requirement. Our coverage addresses financial loss from cyber events – including loss of hire and physical damage – while our modular policies and preparation services help clients meet new regulatory standards. With Beazley Security's layered approach, technical defences and crew readiness are strengthened, supporting proactive risk management in a rapidly changing threat landscape.

beazley