# Cyber Risk and Resilience for Asia Pacific's Marine Industry

# Key Takeaways

1 Digital technologies are transforming Asia Pacific's maritime industry, but they also create new cyber risk exposures.

2 Practical guidance, new regulations and industry initiatives are helping operators take steps to strengthen cyber resilience.

3 Insurers are now offering more flexible and fit-for-purpose solutions to address these exposures.

As a region that is home to many of the world's busiest container ports, shipping is the lifeblood of trade in Asia Pacific (APAC). With vessels and terminals becoming more connected through satellite communications and digital logistics platforms, they are also more exposed to cyber attacks. Threats can range from spoofing navigation systems to ransomware shutting down critical shoreside infrastructure.

For operators, customers and insurers, the question is no longer whether these incidents will occur, but how well prepared the industry is to withstand them. As Andrew Mahony, Head of Cyber Solutions for Aon in Asia notes, the market has reached a turning point. "We've now seen underwriters grow their appetite," he says. "They're willing to be more creative and flexible in covering risks that once seemed almost uninsurable." Insurance, once prohibitively expensive in this space, is now more accessible and better aligned with the industry's real exposures."

## How the Cyber Risk Landscape is Evolving

Cyber attackers adapt their methods to their targets. The maritime industry is no exception, with navigational spoofing now posing a major risk. "The most visible threat we've seen in the news is spoofing — basically distorting and impersonating GPS signals," says Oliver Miloschewsky, Regional Director and Head of Shipping for Aon in Asia. "In the congested shipping lanes or politically sensitive waters of APAC, this misleading positioning data can create serious safety risks, and it raises complex questions regarding liability when these incidents occur."

On shore, ports and logistics operators face ransomware and IT-focused attacks. Business interruption coming from these attacks is particularly damaging in Asia, where a single day of downtime at a hub such as Singapore or Shanghai can cause a ripple of impacts across global supply chains. "Criminals single out these targets because they have more leverage when organisations can expect to suffer such significant losses due to system disruption," says Mahony.

Regulation struggles to keep pace with the speed of these evolving risks. International frameworks such as the IMO cyber risk management resolution[1], BIMCO's industry guidelines[2], IACS' new requirements for ship design[3], and the EU's NIS2 directive[4] all provide guidance on cyber protection standards. Yet adoption and enforcement vary widely across APAC. "In APAC you're dealing with a huge spread of regulatory maturity," says Miloschewsky. "Some markets are very advanced, others are still developing, and that makes consistency a real challenge."

[1] International Maritime Organization, Maritime cyber risk, accessed September 2025

[2] BIMCO, Guidelines on cyber security onboard ships, 14 November 2024

[3] International Association of Classification Societies, IACS adopts new requirements on cyber safety, accessed September 2025

[4] European Commission, NIS2 Directive: securing network and information systems, 1 July 2025

### Steps to Build Cyber Resilience

It is critical companies treat cyber threats as part of their entire risk management strategy rather than a separate concern. Resilience begins with identifying where vulnerabilities exist across onboard systems, port infrastructure and digital supply chains. In APAC, the range of jurisdictions where operators are active means these assessments are rarely straightforward.

“Firstly, organisations must go through a consulting exercise to get a grip on what the exposure is and who is liable,” says Mahony. “Once exposures are mapped, organisations can make informed choices about mitigating risks internally, passing them on contractually, or transferring them through insurance.”

For Miloschewsky, an integrated perspective on these risks is essential. “This is about how cyber fits into broader risk-management plans,” he says. “In practice, that means treating cyber risk not as an isolated technical issue but as part of the wider business continuity framework.”

> “
>
> For fleets operating across Asia Pacific, consistency in cyber risk planning makes the difference between reacting to incidents and building real resilience.
>
> **Oliver Miloschewsky**
> Regional Director and Head of Shipping, Asia

### How Insurance Solutions are Meeting the Marine Market

Insurance solutions for the specific risks the marine industry faces have matured significantly. In the past, marine policies excluded or overlooked cyber triggers, while cyber policies did not always extend to shipboard operations. This left operators uncertain about their coverage for cyber incidents.

Today, there are far more options available. Marine programs can be adapted to recognise cyber events that cause both physical damage or loss of hire. Stand-alone cyber policies can cover office and port systems, as well as offering expert crisis response services to help investigate and contain incidents. Where gaps still exist, specialist solutions are now emerging to bridge them.

To identify solutions that are the best fit, Mahony recommends exploring which specific areas have been left uninsured. "Between core marine policies and a cyber policy, are there any areas of exposure that should be covered and what are the solutions to address that?" he says. "The answer increasingly lies in tailored combinations of cover, supported by those insurers who now better understand the sector."

> "
>
> Coverage has expanded to address business interruption, system failures and third-party liabilities, giving shipowners a broader set of tools to manage cyber exposure."
>
> **Andrew Mahony**
> Head of Cyber Solutions, Asia

### Resilience Across the Industry

APAC's diversity means solutions must remain flexible. A company trading mainly between Japan and Korea faces different obligations from one serving ports across Southeast Asia. These dynamics highlight the value of expert partnerships in connecting global frameworks with regional needs and securing solutions that best fit exposures.

By taking this approach, operators in the region can protect vessels and infrastructure, cargo and customers and keep global supply chains efficient, reliable and secure — even as cyber threats evolve.

## About Aon

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues provide clients in over 120 countries with the clarity and confidence to make better risk and people decisions that help protect and grow their businesses.

Follow Aon on LinkedIn, X, Facebook and Instagram. Stay up-to-date by visiting Aon's newsroom and sign up for news alerts here.

**aon.com**

The information provided in this publication is current as at the date of publication and subject to any qualifications expressed. Whilst Aon has taken care in the production of this publication and the information contained has been obtained from sources that Aon believes to be reliable, Aon does not make any representation as to the accuracy of information received from third parties and is unable to accept liability for any loss incurred by anyone who relies on it. The information contained herein is intended to provide general insurance related information only. It is not intended to be comprehensive, nor should it under any circumstances, be construed as constituting legal or professional advice. You should seek independent legal or other professional advice before acting or relying on the content of this information. Aon will not be responsible for any loss, damage, cost or expense you or anyone else incurs in reliance on or use of any information in this publication.

## Contact Us

**Oliver Miloschewsky**
Regional Director and Head of Shipping, Asia
oliver.miloschewsky@aon.com

**Andrew Mahony**
Head of Cyber Solutions, Asia
andrew.mahony@aon.com

All images courtesy of Goldwind Australia.