WHITEPAPER

Cyber risks in marine and transport

Understanding digital threats, their impact on claims, and the value of a coordinated response

Crawford®

Executive Overview

Digital systems underpin modern shipping and logistics. From vessel navigation and terminal operations to cargo release and payment instructions, goods move through a network of connected technologies and trusted information exchanges.

The connections also create opportunities for disruption and fraud. Compromised credentials can allow criminals to collect a container. A convincing email can divert a shipment. Ransomware can interrupt terminal operations, delaying cargo far beyond the initial point of attack. Artificial intelligence adds to the challenge by making fraudulent documents and communications easier to produce and harder to recognise.

For marine insurers and transport businesses, understanding these exposures is an essential part of investigating losses and managing recovery.

Physical incidents can also damage digital infrastructure or interrupt access to critical systems. Storm damage, structural failure or a vehicle accident may therefore require both a physical assessment and a review of the affected technology. Establishing how the systems failed is central to understanding the loss.

Why marine cybersecurity matters

Marine and transport operations depend on both information technology (IT), which manages data and communications, and operational technology (OT), which monitors or controls physical equipment. An incident affecting either can have consequences for cargo, vessel safety and business continuity.

The exposure extends across organisations. A shipper may rely on a haulier's identity checks, a terminal's release procedures and a third party's tracking platform within a single cargo movement. A weakness at any of these points can undermine otherwise effective controls.

Cyber incidents can result in:

- Cargo theft, misdelivery or loss of sensitive shipment information.
- Disruption to vessel movements, terminal operations and onward transport.
- Financial losses from fraudulent payments, interrupted trading and recovery costs.
- Safety concerns where navigation, monitoring or control systems are affected.

How digital weaknesses can lead to marine losses

The following scenarios illustrate how failures in digital security and verification can affect cargo movements and claims.

CONTAINER THEFT THROUGH COMPROMISED RELEASE PINS

LOAD THEFT THROUGH FALSE HAULIER IDENTITIES

AI-ASSISTED DOCUMENT AND COMMUNICATION FRAUD

COMPROMISED SMART CONTAINERS AND CONNECTED DEVICES

1

CONTAINER THEFT THROUGH COMPROMISED RELEASE PINS

Criminals who obtain a valid container release PIN may be able to collect cargo by presenting it as evidence of authority. Where the release process relies on the PIN alone, possession of the code can be mistaken for proof of identity.

The investigation needs to establish how the PIN was obtained, who could access it and what checks were completed before release. Compromised systems, social engineering and insecure sharing of credentials may all be relevant.

2

LOAD THEFT THROUGH FALSE HAULIER IDENTITIES

Fraudsters can impersonate legitimate hauliers using copied websites, company details and email addresses with subtle alterations. A shipper may believe it has appointed a trusted transport provider, only to hand the cargo to criminals.

These losses highlight the importance of independently verifying the appointed haulier and collection arrangements. Familiar branding or a plausible email exchange is insufficient evidence of identity.

3

AI-ASSISTED DOCUMENT AND COMMUNICATION FRAUD

AI can help criminals produce convincing false bills of lading, delivery instructions and payment requests. Fraudulent communications may imitate the language and presentation of an established business contact, making discrepancies less obvious.

The issue is not simply whether a document looks authentic. Investigators need to establish its origin, whether instructions were altered and how any changes were authorised. Requests to redirect cargo or amend payment details warrant particular scrutiny.

4

COMPROMISED SMART CONTAINERS AND CONNECTED DEVICES

Smart containers and other Internet of Things (IoT) devices monitor conditions such as temperature, humidity, movement and door status. Their value depends on the reliability and security of the information they collect and transmit.

Compromised devices or platforms could expose shipment locations, allow monitoring data to be altered or undermine alerts about cargo conditions and unauthorised access. In a claim, the integrity of that data may be as important as the physical condition of the cargo.

Where to look for exposure

Cyber risk should be considered wherever digital information authorises an action, controls equipment or provides evidence of what happened. Key areas include:

- **Ports and terminals:** operating systems, cargo release platforms and quayside networks.
- **Vessels:** navigation, engine controls and vessel-to-shore communications.
- **Inland transport**: telematics, fleet management and digital haulier appointment processes.
- **Cargo documentation and monitoring**: electronic bills of lading, tracking platforms and connected sensors.
- **Marine infrastructure:** digital controls for bridges, locks and coastal assets.
- **Third-party connections:** software providers, remote access arrangements and shared supply-chain platforms.

Cyber Risk Exposure Areas

PORTS AND TERMINALS

VESSELS

INLAND TRANSPORT

CARGO DOCUMENTATION AND MONITORING

MARINE INFRASTRUCTURE

THIRD PARTY CONNECTIONS

The review should consider how these systems connect and who controls them. A secure internal network may still be exposed through an external provider, compromised user account or poorly controlled access route.

Legal and regulatory considerations

A marine cyber incident may involve data protection, security and incident-reporting obligations. The applicable duties depend on the organisation, the services it provides, the information affected and the jurisdictions involved.

Early assessment should establish which obligations apply and who is responsible for the response. Where several supply-chain partners are involved, system ownership, access arrangements and contractual responsibilities should be examined rather than assuming responsibility rests with a single party.

In the UK, two areas deserve early attention:

- **Personal data breaches:** Where a breach meets the notification threshold under the UK GDPR, the controller must notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of it. Not every cyber incident is a reportable personal data breach.
- **Essential services:** Transport operators within the scope of the Network and Information Systems Regulations have security and incident-reporting obligations. These requirements apply to qualifying operators, rather than every organisation involved in shipping or logistics.

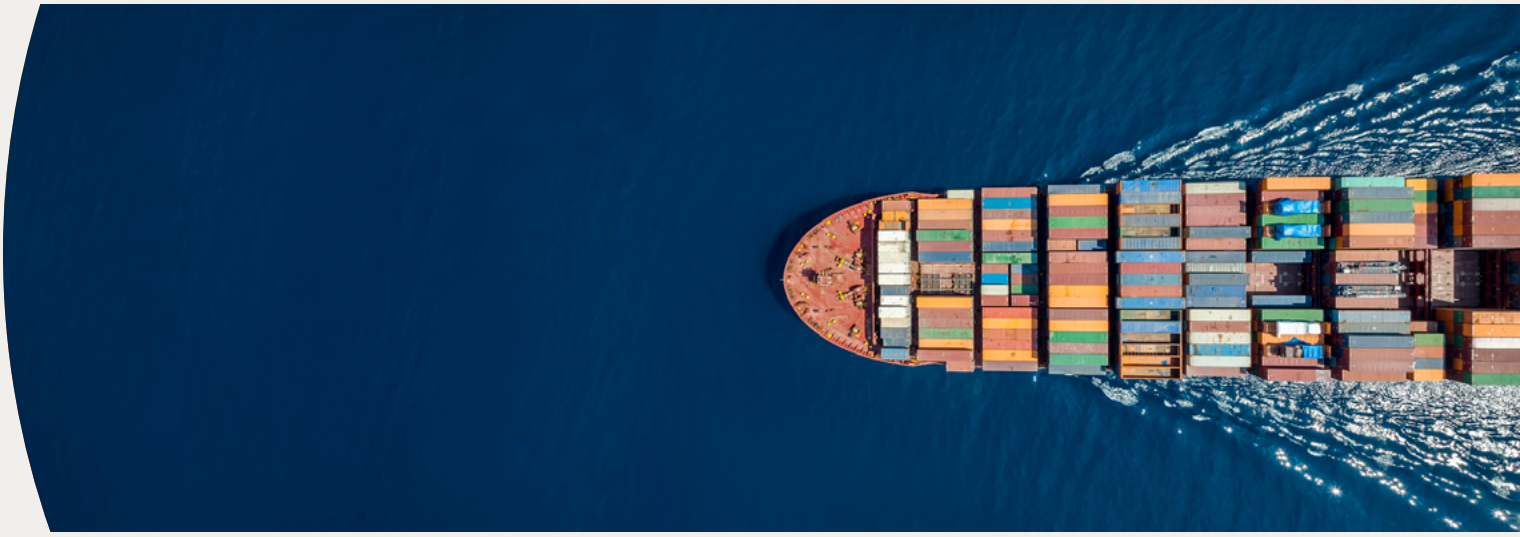
Investigating the loss and planning recovery

Restoring access to a system is only part of recovery. An incident may leave uncertainty about the reliability of cargo records, the integrity of operational data or the extent of disruption. Those questions can affect both the return to normal operations and the assessment of the claim.

A coordinated marine and cyber investigation should address:

- **Cause and extent:** Establish the entry point or failure mechanism, the systems affected and whether the incident remains active.
- **Evidence:** Preserve relevant logs, communications, release records and other digital material alongside the physical evidence.
- **Operational impact:** Establish pre-incident functionality and identify which activities were interrupted, for how long and with what consequences.
- **Financial loss:** Assess interruption losses and recovery costs against the available operational and financial records.
- **Recovery**: Support proportionate containment and restoration, taking account of operational dependencies and safety requirements.

Marine specialists bring an understanding of cargo handling, vessel operations and transport practices. Cyber specialists examine the systems, access routes and digital evidence. Bringing those findings together helps explain how the incident developed and supports a clear, evidence-based assessment of the loss.



How Crawford supports marine and transport claims

Crawford's marine surveyors and adjusters draw on in-house cyber expertise to investigate incidents involving both physical operations and digital systems. Early engagement helps identify the nature of the exposure and the specialist support required.

Depending on the incident, our support includes:

- Triage of suspected system compromise and assessment of operational and data exposure.
- Review of IT and OT vulnerabilities relevant to the loss.
- Examination of digital identities, documentation and suspected AI-assisted fraud.
- Business interruption and financial loss quantification.
- Recovery and remediation planning, with digital forensic specialists and other partners where required.
- Technical reporting to support insurers and clients, including coordination with regulatory advisers where appropriate.

Our marine and cyber teams work together through investigation, mitigation and reporting. This gives insurers and clients a connected assessment of the digital incident and its practical consequences for vessels, cargo and transport operations.

Early recognition of the cyber element can shape the course of a claim. It helps teams preserve evidence, make informed recovery decisions and understand the full extent of the loss.

About Crawford & Company®

For over 85 years, Crawford has led the industry through a relentless focus on people and the innovative tools that empower them.

10K employees | **50K** field resources | **70** countries | **$20B** claims managed annually

Crawford®

Learn more at
www.crawco.com