



ESG

# CYBER RISKS AND THE DIGITAL REVOLUTION: A SHIPPING PERSPECTIVE



INFORMED INSURANCE  
SEPTEMBER 2023

**dgcb**  
**DAC BEACHCROFT**  
Member of **Legalign Global**

# Cyber Risks and the Digital Revolution: A Shipping Perspective

Finally, it seems the cyber threat penny has dropped, with most businesses now working hard to protect their assets from hackers. For the shipping sector, where does that threat sit among the myriad of competing priorities?

It is estimated that, in the first half of 2022 alone, 2.8 billion malware and 255 million phishing attacks were reported across the world with 71% of businesses admitting to falling victim. When you consider these are merely the reported attacks, you start to get a sense of the scale of the threat to the global economy.



## Hunting weakness

As entire sectors wake up to the ever-present cyber threat, the criminal gangs perpetrating the majority of attacks are turning their attentions to the less protected to maintain their income, as Tom Evans, International Wording's Lawyer at marine and cyber insurance specialist Beazley, explains.

"These gangs work on a volume basis so they will always go after the slowest in the herd, adapting and targeting wherever they see weakness," he says.

"The hacking community understands that financial services, a key target, has got its security act together, so they are now going after industries and organisations that have not got the right protection in place."

One of these new targets is the shipping sector, estimated to be responsible for facilitating around 80% of the world's trade. The threat is large, systemic and increasing in likelihood. But while awareness of the cyber threat is growing in the sector, other developments are increasing the threat posed.

## Shipping's digital revolution

Over recent years, the shipping industry has undergone something of a digital revolution. Operators are turning to tech to influence everything from tracking a ship's performance to securing greater efficiency on shipping routes. But one of the key drivers for this digital transformation is a need to hit an industry-wide net-zero target by or around 2050.

"The need to decarbonise and to do it quickly is driving the adoption of digital tools to optimise shipping operations," says Joanne Waters, Legal Director at DAC Beachcroft.

"In addition, new regulations coming in January 2024 require all ports to be able to exchange data with ships electronically. The connectivity required to achieve that brings cyber risks into play."

The sector finds itself in something of a bind. It has to digitise to satisfy regulatory, environmental and, increasingly, commercial demands but while it does so, the cyber threat grows and adapts.

## The risks are the same

Despite this, the cyber risks the sector faces are really no different from those facing any other business.

"Broadly speaking, it is the same risks," says Evans.

"While you have operating tech in the marine industry, it's the head office risk that is the big one. What we see routinely is the exact same ransomware threats that would apply to a bank or retailer with the most obvious example being the attack on Maersk, one of the world's largest shipping organisations."

Since the Maersk hack in 2017, other major shipping companies such as Cosco, MSC and CMA CGM have all experienced serious attacks and the Port of Los Angeles said it now manages double the number of attacks it did just a few years ago, tackling 40 million ransomware, malware and phishing attempts every month.

"The need to decarbonise and to do it quickly is driving the adoption of digital tools to optimise shipping operations."





## IT and OT

But while the type of threat the shipping sector faces may not be new, there are some nuances that make it more difficult to manage.

"The threats are split between information technology (IT) and operational technology (OT)," says Hans Allnutt, Partner at DAC Beachcroft.

"Operational technology includes control systems on the ship and on shore, and this technology is now increasingly connected and remotely accessible whereas before it might have been in a closed loop. This brings greater cyber risk complexity to this sector compared to other sectors that might only rely on information technology, not least because of the challenge to responding to hacked technology out at sea."

With the blockage of the Suez Canal a recent, sore and expensive memory, the idea of hackers taking control - or indeed simply removing control - of a large container ship or tanker is enough to make marine insurers' blood run cold. But while it is the OT risks that bring the most obvious interruption to ship movements, it is the IT systems that create the most likely and greatest operational vulnerability.

According to a survey conducted by DNV, an advisor to the shipping sector, nearly a third of maritime professionals have experienced an IT attack while less than a quarter have experienced an OT attack.

"It's easier to hack the shipping company's headquarters, encrypt everything and then demand a ransom, than it is to hack the ship itself" explains Allnutt.

Firms should also avoid the trap of thinking that they are not an attractive target to cyber criminals.

"A company may not be targeted themselves but simply have a common technology vulnerability that happens to be exploited. Systems attacks like NotPetya and WannaCry demonstrate that business across the globe can be affected by attacks that are launched against other unrelated firms. If someone decided to exploit a vulnerability common to shipping and control systems, that could be devastating globally" says Allnutt.

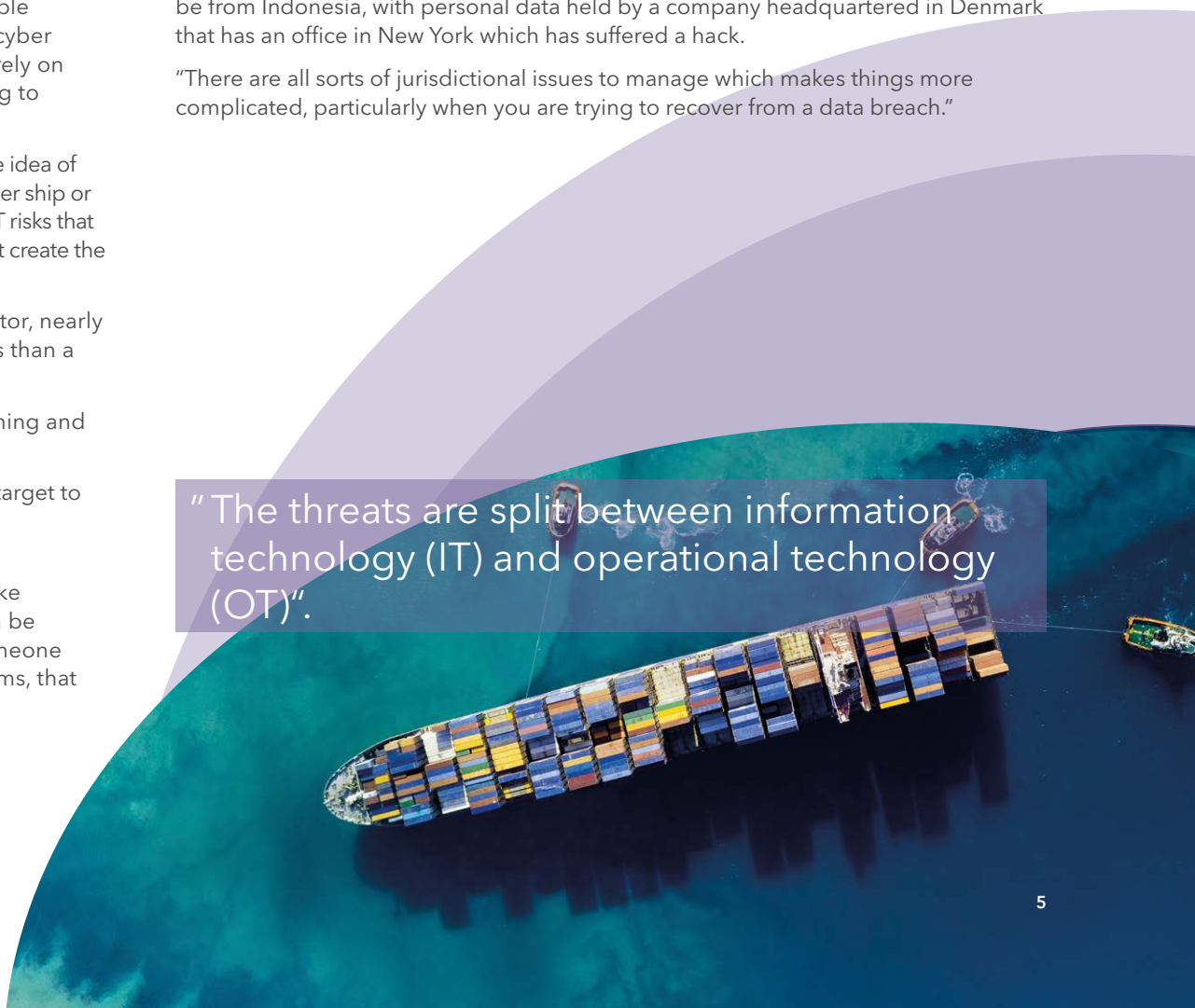
## Global reach

It's not just the tech and connectivity that makes managing cyber risks in shipping particularly complex. It's the very nature of the industry itself.

"Shipping companies are more complicated and more interesting because they are truly global enterprises," says Evans.

"They will hold personal data on people from all over the world. A crew member may be from Indonesia, with personal data held by a company headquartered in Denmark that has an office in New York which has suffered a hack.

"There are all sorts of jurisdictional issues to manage which makes things more complicated, particularly when you are trying to recover from a data breach."



"The threats are split between information technology (IT) and operational technology (OT)".

## Mind the gap (in cover)

So what can the shipping sector and the insurance industry do in response? The awareness is building from historical attacks and with the impetus from regulators but, in an industry where margins are tight and priorities are plentiful, it can be difficult to know where to focus the available resource, as Waters explains.

"It's more about identifying the gaps in cover. Shipping has quite complex insurance requirements and the risks are often spread across various products. Operators need to ask themselves the extent to which any existing cover provides protection for the new risks that arise from the adoption of digital tools and increased connectivity".

## Awareness and priorities

While it is clear that shipping has some significant cyber vulnerabilities, it may not be as bad as some fear.

"Those that have improved their cyber risk management are completely switched on, know where the risks lie, understand their risk profile and they manage it well. But there are still a number of smaller organisations that could do more," says Evans.

"The industry as a whole is taking it far more seriously and there has been significant leadership from the International Maritime Organization which has helped bring the cyber concern to the forefront."

Awareness is a critical step in the evolution of cyber protection: and the good news is that it is growing and growing fast. But just because operators are aware, doesn't mean they have the means to respond.

"There is an awareness that it is a risk but the question is where responding to that risk sits in their priorities," says Waters.

"The majority of shipowners are SMEs, operating with a couple of ships. They may not have a dedicated IT department let alone a Chief Information Security Officer. Despite their growing awareness that the introduction of more tech translates into increasing levels of risk, the ability to invest in greater cybersecurity depends on what sector you are in and whether that sector is making money."

Insurers will be encouraged to learn that, despite all the competing priorities fighting for attention, cyber risk remains one of the most pressing for operators. According to one survey, cyber risks are the number two threat, behind natural catastrophes and ahead of 'traditional' piracy.

"There is a growing awareness," says Evans, "and it is moving in the right direction. There are many organisations that take the threat seriously and understand where the risks are coming from."

He adds that commercial imperatives, driven by the larger firms, will also increase awareness and use of risk mitigation: "It would be entirely reasonable for them to stipulate a certain cyber security standard before they would outsource or partner with an SME organisation," says Evans.

While systemic risk very much exists, the likelihood of it manifesting is remote. Of far more concern are run of the mill attacks, the same attacks that every other part of the economy has been fighting for years.

At least this means there is a proven insurance model, one that seeks to prevent as well as manage incidents, and it seems that shipping, which regularly manages more physical risks than any bank ever has, is more suited to this approach than many others. The threat is there but so too is the protection.

**Contributors:**

**Hans Allnutt**

hallnutt@dacbeachcroft.com  
Partner, DAC Beachcroft, London

**Joanne Waters**

jowaters@dacbeachcroft.com  
Legal Director, DAC Beachcroft, London

**Tom Evans**

International Wordings Lawyer, Beazley

**Click below to read our whole suite of new thought leadership:**

- [People, Planet, Profit: How to Marry Purpose and Value in the Pursuit of Sustainability](#)
- [Heat Rises on Climate Change Litigation Risk](#)
- [Biodiversity Comes to the Fore: Toward Nature-Positive Outcomes](#)
- [Geopolitical Risk in Latin America: Shock Disruptions, Political Blurring and a Multipolar World](#)



[insurance.dacbeachcroft.com](https://insurance.dacbeachcroft.com)

[dacbeachcroft.com](https://dacbeachcroft.com)

✕ Follow us: @DACBeachcroft

in Connect with us: DAC Beachcroft LLP

DAC Beachcroft publications are created on a general basis for information only and do not constitute legal or other professional advice. No liability is accepted to users or third parties for the use of the contents or any errors or inaccuracies therein. Professional advice should always be obtained before applying the information to particular circumstances. For further details please go to [www.dacbeachcroft.com/en/gb/about/legal-notice](https://www.dacbeachcroft.com/en/gb/about/legal-notice). Please also read our DAC Beachcroft Group privacy policy at [www.dacbeachcroft.com/en/gb/about/privacy-policy](https://www.dacbeachcroft.com/en/gb/about/privacy-policy). By reading this publication you accept that you have read, understood and agree to the terms of this disclaimer. The copyright in this communication is retained by DAC Beachcroft. © DAC Beachcroft 2023. Prepared September 2023.