Cyber security risks for charterers

Cyber security has been a growing concern for the shipping industry in recent years. As the use of technology on board ships increases, so does the risk of cybercrime. This article focuses on the effect of cybercrime on charterparties.

Atousa Khakpour
Claims Executive
T +65 6506 1945
E atousa.khakpour@ctplc.com

What is cybercrime?

A cybercrime is the intentional infiltration of a technology system by a third party without consent. For charterers, the major risks are financial loss and data theft, which can lead to reputational damage, lawsuits, business interruption and regulatory action.

Diversion of payments

The fraudulent diversion of hire and freight is becoming increasingly common. Hackers infiltrate an email system to find out the details of business contacts. They then email the charterer impersonating the accounts department of a payee to redirect payment, either attaching an invoice with a specified bank account or specifically requesting hire to be paid into a different account than normal. Often the email address used by the hacker is almost identical to the email address of the true counterpart, with only a small variation which can easily go unnoticed.

It is not always apparent that a charterer has fallen victim to cybercrime until the owner complains that hire is unpaid. Generally, hire is only considered paid when the funds have been received in the owner's designated bank account. Therefore, if the charterer makes a payment which does not reach that account within the payment date, the charterer will be in breach of the charterparty. The owner may then be entitled to withdraw the vessel from service if the charterer does not pay again pursuant to the terms of any anti-technicality clause. This can result in the charterer paying twice.

Protecting your position

Whilst members cannot always prevent a cyber-attack from occurring, members can seek independent legal advice to protect their position contractually, for example, by:

- making 'Cyber Event' a defined term
- including a clause allowing more time to pay in the event of a Cyber Event
- including 'Cyber Event' as an off-hire event in the off-hire clause
- excepting 'Cyber Event' from laytime and demurrage.

A 2016 PWC Global Economic Crime Survey recorded cybercrime as 'the fastest growing global economic crime', with Forbes projecting the cost of cybercrime to reach $2 trillion by 2019.

Spotting cybercrime
Members should remain alert to the risk of cybercrime at all times.

- Always check email addresses carefully, especially when discussing payment details.
- Be aware. Treat any changes in the communication style or form with suspicion.
- Cross-check any bank account provided in the email against the bank account details contained in the charterparty.
- If you have any suspicions, do not respond by email as it may be intercepted.
- Always telephone the payee to verify the bank details.

BIMCO has published guidelines aimed at preventing cyber security breaches. Though the guidelines focus on shipboard risks, they nonetheless highlight the need for senior management to co-ordinate risk assessments and develop contingency plans. The guidelines can be found on the BIMCO website.

Club cover
Costs incurred in respect of a charterparty dispute relating to cybercrime can be covered under the club's Defence cover, subject to the war risks exclusion found in P&I rule 4.3.

Where charterers incur a P&I liability arising from cybercrime, poolable P&I cover can respond, subject to the paperless trading and war risks exclusions.

For further information on cyber risks and implications on club cover, please refer to the club's Standard Bulletin March 2017 edition.

Award-winning global maritime cyber security awareness campaign, Be Cyber Aware at Sea, has collaborated with Fidra Films to launch a new film which aims to highlight the vital and increasing importance of cyber security across the maritime industry. The project has been supported by The Standard Club, along with NSSLGlobal, a global maritime satellite communications provider, Oil Companies International Marine Forum (OCIMF) and Teekay.

The film uses real-life case studies to highlight how easy it is for cybercriminals to target individual employees, who are often the weakest link in the security chain. Lots of people still fail to spot the signs of simple phishing emails, and accidentally give away secure information to hackers via email or social media. Even something as simple as charging a phone using the ECDIS[1] could allow hackers to gain access to the ship's navigation system. The video therefore focuses on tips to avoid being a target for cyber criminals.

This release is particularly timely given the recent reports of a widespread cyber attack affecting companies around the world, including Maersk.

The video is freely available on youtube. Members are encouraged to distribute it to their fleets and reinforce its messages.

Members requiring further information on this topic should direct their enquiries to either their usual contact at the club or to the authors of this article.

[1] Electronic chart display and information system.