Cyber risks and P&I insurance implications

As navigation and propulsion systems on board ships and offshore units become increasingly dependent upon computer technology, the threat of cyber attack has emerged as a potentially significant exposure for the maritime sector. In this article, we outline how standard P&I cover generally operates in respect of shipboard cyber risks.

Rupert Banks
Regional Claims Director
T +65 6506 2882
E rupert.banks@ctplc.com

> In an age where cyber threats are becoming increasingly prevalent, shipowners are urged to be alert to the vulnerability of ships to cyber attacks.

Vulnerability to cyber attacks

Modern vessel navigation has become increasingly dependent upon computers and computer software. Bridge systems such as ECDIS, AIS and GPS[1] are all now important and integral features of a ship's ability to navigate safely. In addition, DP[2] systems on board ships employed in the offshore sector are critical in ensuring that they can manoeuvre with precision even in harsh sea conditions.

All of these systems have been identified as being vulnerable to cyber attack. In the event that one or more of them were to be compromised, this could lead to a member incurring P&I liabilities such as collision, personal injury, property damage, pollution or wreck removal.

How would standard P&I cover operate in such a scenario?

Poolable P&I cover

Other than the exclusion relating to paperless trading, there is no express cyber exclusion in the club's rules. As such, a member's normal P&I cover will continue to respond to P&I liabilities arising out of a cyber attack so long as the attack in question does not constitute 'terrorism', 'a hostile act by or against a belligerent power' or another war risk excluded under rule 4.3 of the club's rules.

Whether or not a cyber attack constitutes an act of terrorism for the purposes of the rules will generally depend upon the motivation behind it. In the context of war risks, terrorism is broadly understood to denote acts aimed to kill, maim or destroy indiscriminately for a public cause. Accordingly, if, for example, a cyber attack were to be perpetrated by an individual or group for the purposes of causing general disruption and for no public cause, then this would be very unlikely (without more) to constitute terrorism for the purposes of the rules and a member's cover will respond in the normal manner. However, in the event of any dispute as to whether or not an act constitutes terrorism, the club's board is given the power under rule 4.3 to decide and such decision shall be final.

If a cyber attack were to be executed against a ship by a government or organised rebels in a period of war or civil war, the war risks exclusion in the rules would be engaged.

A 'hostile act by or against a belligerent power', however, is not defined in the rules and, unlike terrorism, the club's board does not have the same discretion to ultimately decide what this means. However, such acts have generally been deemed by courts to arise in circumstances of war or civil war and to be perpetrated by governments or organised rebels.

Accordingly, if a cyber attack were to be executed against a ship by a government or organised rebels in a period of war or civil war, the war risks exclusion in the rules would be engaged. Otherwise, and subject to the remainder of the rules, a member's standard P&I cover could respond.

Relevant extensions

In the event that a particular cyber attack does constitute 'terrorism', 'a hostile act by or against a belligerent power' or another excluded war risk, then the club's excess P&I War Risks clause (and, for special risks, the War Risks clause for additional covers) may respond but not to the extent that the cyber attack involves the use or operation of a computer virus as a means for inflicting harm. The intent to cause harm will be implicit as the cyber attack will already have been deemed to be terrorism or another war risk in order for the war risks exclusion in the P&I rules to have been triggered. Accordingly, these extensions will not respond in those particular circumstances.

Where a cyber attack does constitute an excluded war risk under the P&I rules and is excluded under the excess P&I War Risks clause (and under a member's primary war cover), the club's Bio-chemical Risks Inclusion clause provides a limited buy-back (for owned entries only) of up to $30m in respect of liabilities to crew as well as sue and labour expenses where the liability is directly or indirectly caused or contributed to by or arises from the use of any computer, computer system, computer software program, malicious code, computer virus or computer process as a means of inflicting harm.

However, cover under this extension is subject to certain exclusions, notably liabilities arising out of the use of the ship or its cargo as a means of inflicting harm. As such, in extreme cases where, for example, a malicious third party were to hack into the navigation controls of a ship and then deliberately steer the ship into collision with another ship or object, those crew liabilities and sue and labour expenses that would otherwise be covered under the clause would be excluded given that the ship would have been used as a means of causing harm.

Conclusion

In an age where cyber threats are becoming increasingly prevalent, shipowners are urged to be alert to the vulnerability of ships to cyber attacks. The above is a summary of how standard P&I cover generally operates in respect of shipboard cyber risks. Naturally, each case will be considered individually based on the facts. Should members have any queries, please do not hesitate to approach your usual club contact.

1 Electronic Chart Display and Information System, Automatic Identification System and Global Positioning System, respectively.
2 Dynamic Positioning.