MANAGING CYBER RISKS AND THE ROLE OF THE P&I CLUB: AN OVERVIEW

ABS Group

THE AMERICAN CLUB 1917

October 2020

Managing cyber risks and the role of the P&I club: An overview

Introduction

Generally speaking, and in contrast to most other forms of marine insurance, the rules (or basic conditions of cover) of International Group P&I Clubs (IG) do not exclude claims arising from cyber incidents, unless such an incident were considered to be an act of war or terrorism. Accordingly, regular Group club P&I cover would be available for the consequences of a non-war or terrorism related cyber incident. This might arise, for example, from a simple onboard computer malfunction, from a breakdown unintentionally caused by remote intervention in onboard systems, or even from an act of sabotage by a disgruntled former employee. In the circumstances, being part of the IG, and as discussed in further detail in the remainder of this Overview, the American Club has a particularly salient interest in cybersecurity. It is hoped that this joint initiative with ABS Consulting will place many exposures associated with cybersecurity in context, and assist with building systems to avoid them.

Crew training and awareness are crucial, as the most common way for cyber criminals to attack is through inadequately trained individuals. A 2018 survey revealed that 47% of the seafarers questioned stated they had sailed on a vessel that been a target of a cyber attack. Regrettably, only 15% of those seafarers acknowledged having received at least some cybersecurity training provided by their manning agent. Unfortunately, most of the cyber training was not specific either to the company or to the ship. Additionally, only 33% of those seafarers stated that the company with which they were employed had a policy of regularly changing passwords for password required systems onboard ship. There is clearly room for improvement and a need for preventative measures to reduce or eliminate cyber vulnerability through proactive awareness training of seagoing personnel.

Although there are no explicit cyber exclusions in the American Club's rules, Members should act as prudent uninsureds and take all steps as are reasonable for the purpose of averting or minimizing any expense or liability that may result from cyber risks. Accordingly, Members should adopt appropriate cyber protection as P&I cover could be prejudiced if shipboard systems are compromised.

The American Club has teamed with its industry partner, ABS Consulting, to publish Safety, Risk and Compliance Management: A Primer on IMO Cyber Risk Management Guidelines to assist in assessing Members' cybersecurity readiness. Furthermore, your Managers have made available to Members exclusively access to a cybersecurity readiness review questionnaire that provides guidance as to actions to consider depending upon Members' level of cyber awareness readiness. Members are encouraged to complete the questionnaire to gain a greater insight into what further actions may be necessary for Members to best address cyber risks both onshore and onboard ship.

How would P&I insurance respond to a cyber risk event once it materializes? What can shipowners do to prevent and mitigate cyber risks in such cases? Each case will depend on its own circumstances and facts. We have created some scenarios for consideration, and provided guidance on P&I and FD&D coverage from a cybersecurity perspective in relation thereto.

Cyber risks affecting ship operations

Cyber risks can create any number of shipboard problems for the Master and crew, such as, but not limited to:

- Distracting the attention of the Master and crew who have other tasks to take care of by creating a backlog of work.
- Backing up files is time consuming and may require sending IT personnel to the vessel to assist adding to costs.
- Loss of historical data of the ship permanently could mean losing vital safety and maintenance records.
- If locked out of applications this could prohibit the vessel from using navigational aids such as tides and currents programs, cargo programs, safety and maintenance programs, alarm systems, chart correction programs and emails. On cruise ships this could include the passenger manifests as well.
- Crew and passenger personal information is at risk of exploitation.
- Loss of control of automated programs such as autopilot, alarms, machinery control panels
- Delay of ship's departure to bring vessel back to operationally safe status.
- Interruption of cargo loading or discharge operations.
- Interruption of navigational or critical machinery systems that could potentially lead to a grounding, collision damage to third party property as well as personal injury and a pollution incident.

Such risk scenarios should be considered by Members in updating their company's safety management system (SMS) when assessing cybersecurity risks. The following case studies provide various scenarios of incidents that can occur, the P&I and FD&D implications and cybersecurity best practices to prevent and mitigate such incidents.

I) Infection of a ship's navigation system or application server

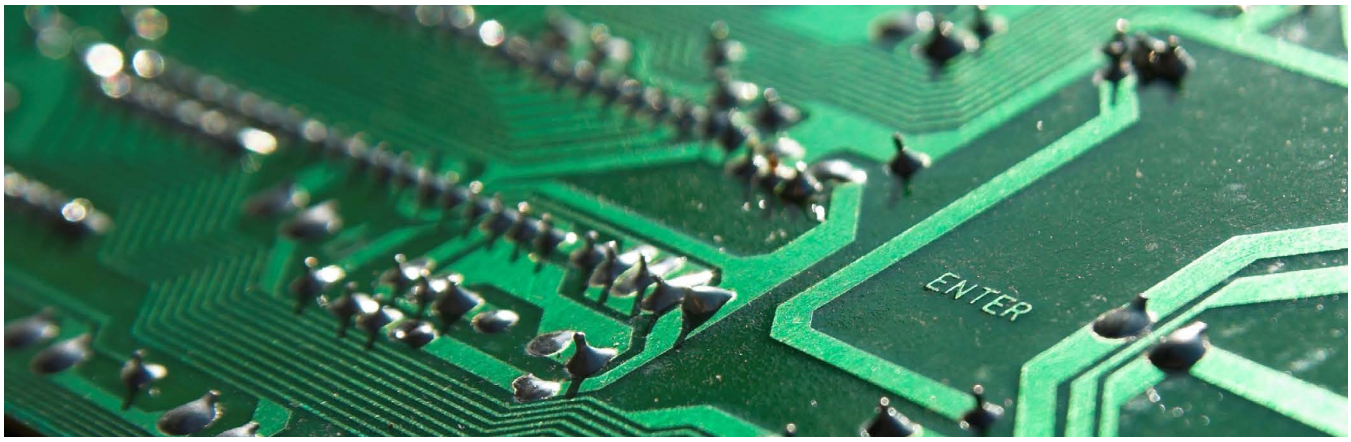
A new-build dry bulk ship laden with cargo was delayed from sailing from the loading port for several days because its Electronic Chart Display and Information System (ECDIS) was infected by a virus. The ship was designed for paperless navigation and was not carrying paper charts. The failure of the ECDIS appeared to be a technical disruption and was not recognized as a cyber issue by the ship's master and officers. A producer technician was required to visit the ship and, after spending a significant time in troubleshooting, discovered that both ECDIS networks were infected with a virus. The virus was quarantined and the ECDIS computers were restored. The source and means of infection in this case are unknown. The delay in sailing and costs in repairs totaled in the hundreds of thousands of US dollars.

Similarly, ransomware infected the main application server of the ship and caused complete disruption of the IT infrastructure. The ransomware encrypted every critical file on the server and as a result, sensitive data were lost, and applications needed for ship's administrative operations were rendered unusable. The incident continued to reoccur even after complete restoration of the application server. The root cause of the infection was a poor company password policy that permitted attackers to successfully infiltrate remote management services. The company's IT department deactivated the undocumented user and enforced a strong password policy on the ship's systems to remediate the incident.

i. P&I and/or FD&D Impact

The vessel was on time charter under an unamended NYPE 1946 form. Clause 15 read as follows:

> *"In the event of loss of time from deficiency of men or stores, fire, breakdown or damages to hull, machinery or equipment, grounding, detention by average accidents to ship or cargo…. or by any other cause preventing the full working of the vessel, the payment of hire shall cease for the time thereby lost."*



Accordingly, the charterer placed the vessel off-hire for the duration of the delays, arguing that the malfunctioning ECDIS (breakdown of equipment) prevented sailing of the vessel, which otherwise was ready to sail with her cargo; full working of the vessel was prevented and the vessel was not fit to perform the service required of her.

Here the shipowner's and the charterer's respective FD&D insurers would aid the Member in regard to the dispute vis-à-vis the off-hire event. Any associated legal costs would be covered by the shipowner's FD&D insurance policy. FD&D insurance provides cover for claims handling assistance and for costs of employing lawyers and experts, as may be necessary to pursue or defend such disputes. However, FD&D does not cover the principal sum in dispute, such as the disputed hire in the instant scenario. FD&D cover is by its nature discretionary in that the P&I club would consider several factors including the merits of the Member's case, quantum of the case, that the expenditure would not be outweighing the aimed beneficial result, and whether the Member acted prudently (i.e. has exercised due diligence to prevent the incident causing the claim).

If, for example, the ship was laden with perishable cargo, such as bananas, significant delays in the voyage could result in ripening before arrival at the discharge port. In that case, the consignee would likely claim damages from the carrier and arrest the vessel for security. To prevent/lift the vessel's arrest, the shipowner's P&I insurer would issue security. Cargo interests' claim here is covered by the P&I club.

ii. Cybersecurity Best Practices: ECDIS virus

The introduction of new cybersecurity procedures is typically easier to plan and implement by focusing on the changes and impacts to people, processes, and technologies. In the ECDIS virus example, the virus could have been prevented by training crew to scan USB drives containing charts updates for viruses before plugging in, updating and following a Management of Change (MoC) procedure to include scanning of all USB drives, and installing anti-virus on the ECDIS or a dedicated USB-scanning computer as technologies to simplify the new procedures.

- Develop policies and procedures regarding the use of removable media
- Develop procedures for protection of risks from service providers' removable media before connecting to the vessel's systems
- Prevent the application of software updates by service providers using uncontrolled or infected removable media
- Install removable media blockers on all physically accessible computers and media ports
- Install intrusion detection system to identify unauthorized use of removable media

- Deliver cyber awareness training; helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to cybersecurity. Existing company procedures for identifying training requirements should be used to assess the benefits and need for:
    - All company personnel to receive basic cyber awareness training
    - Company personnel, who have been assigned cybersecurity risk management duties, to receive a type and level of cyber training appropriate to their responsibility and authority

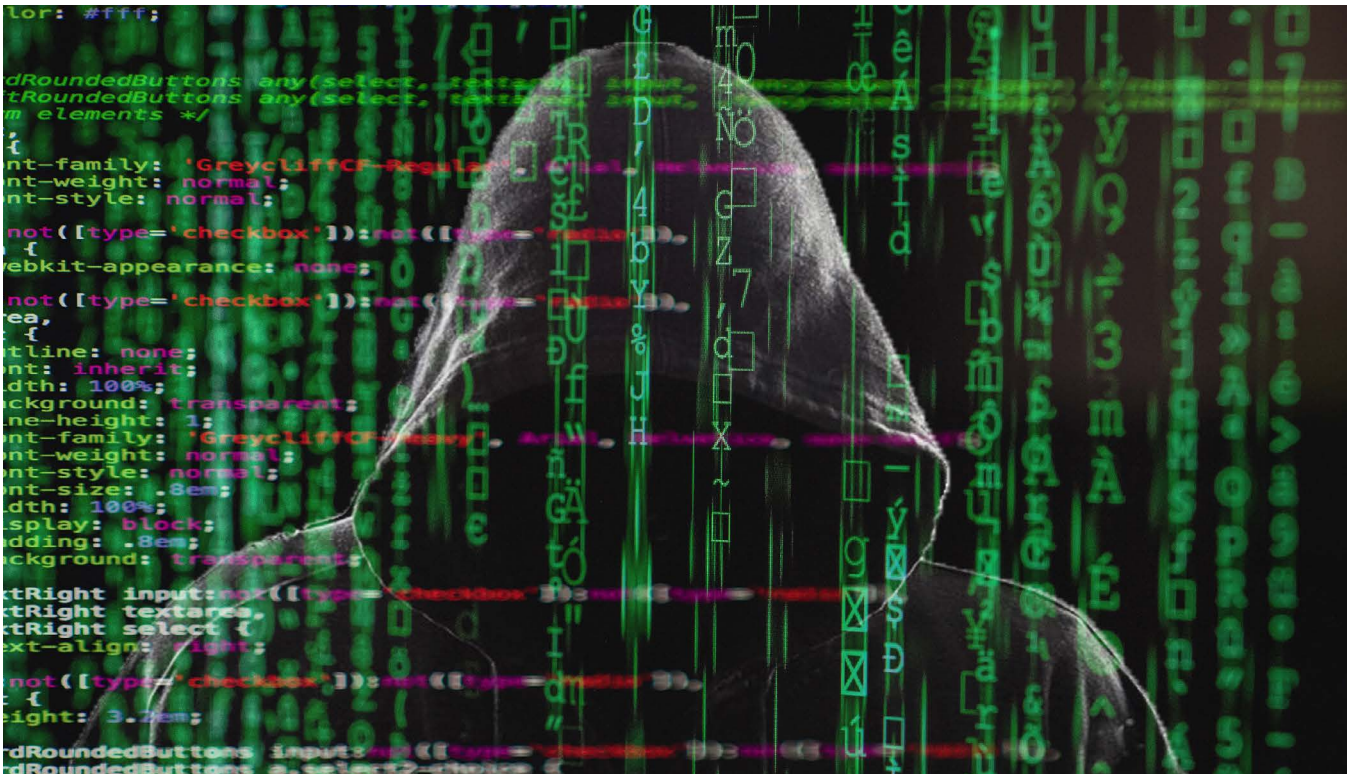
iii. Cybersecurity Best Practices: Ransomware

Ransomware is a specific type of malicious software (malware) that is designed to encrypt a computer hard drive and hold that data "ransom" until the threat actors have been paid. Ransomware is one of the most common forms of malware today. In many cases, large companies pay the ransom to restore access to their critical data. Ransomware cases typically occur on business IT networks and spread from email servers to other servers and computers. When operational technologies (OT) are connected to business IT networks, ransomware proliferates to cyber-enabled control systems. Infections on critical control technologies can have destructive physical effects.

As with other forms of viruses, ransomware can be prevented with updates to cybersecurity practices including people, processes, and technology. In addition to policies, procedures, and training, the technical safeguards listed below are designed to greatly decrease the odds of ransomware infections on critical infrastructure and operational technologies.

- Perimeter defense such as firewalls are important for preventing unwelcomed entry into systems
    - A perimeter firewall between the onboard network and the internet
    - Network switches between each network segment
    - Internal firewalls between each network segment
    - Virtual Local Area Networks (VLAN) to host separate segments
- Password policy
    - Passwords should be strong and changed periodically
    - Default administrator accounts and passwords should not be used
- For insider threats, a combination of the following needs to be applied:
    - Physical security of the ship in accordance with the ship security plan (SSP)
    - Protection of networks, including effective segmentation

- Intrusion detection
- Periodic vulnerability scanning and testing
- Software whitelisting
- Access and user controls
- Appropriate procedures regarding the use of removable media and password policies
- Personnel's awareness of the risk and familiarity with appropriate procedures



II) Hacking of the company's email or business network systems

Cyber hackers gained access to a shipowner's or charterer's email system. At the time of payments to be made, the cyber hackers impersonated the shipowner or charterer leading to payments under the charterparty being misdirected to impersonator's bank account.

Similarly, a shipowner reported that the company's business networks were infected with ransomware, apparently from an email attachment. The source of the ransomware was from two unwitting ship agents, in separate ports, and on separate occasions. Ships were also affected but the damage was limited to the business networks, while navigation and ship operations were

unaffected. In one case, the shipowner paid the ransom.

i. P&I and/or FD&D Impact

In the case of misdirection of payments to hackers, which happens frequently, the risks fall outside the P&I cover because there is no third-party liability encountered in the commercial operation of the entered vessel. The Club would provide assistance within the context of FD&D cover and take legal action in order to recover those misdirected funds. FD&D insurance provides cover for claims handling assistance and for costs of employing lawyers and experts, as may be necessary to pursue or defend such disputes. FD&D does not cover the principal sum in dispute, such as the misdirected funds in the instant scenario. FD&D cover is by its nature discretionary in that the Club would consider several factors including the merits of the Member's case and whether the Member has exercised due diligence in order to ensure that the payment instructions for the proper party had been duly followed.

ii. Cybersecurity Best Practices: Hacking of company's email system

Email incidents may occur because company employees are deceived into sharing information or following instructions in emails. Examples of email incidents include phishing emails. In the first email example the actual attack was due to a phishing email demanding the misdirection of a charterer's payment. The first example was likely caused by a spear phishing attack.

Spear phishing is a more targeted email attack. Spear phishing attacks require that the threat actor learn more about the background and responsibilities of the targeted employee. To perform a spear phishing attack, threat actors will look in social media and attempt to discover as much about employee's personal and professional lives. Once a connection can be established between a person's employer and their job, a threat actor can attack.

In the payment email example, the threat actor sent an email to the employee that included payment instructions to the impersonator's bank account. As threat attacks go to great lengths to appear legitimate, the employee believed that this was the appropriate bank account. The charterer's employee made the payment.

Spear phishing attacks rely on typical

human behavior to occur. Phishing attacks can be prevented by recognizing these attacks and reporting them immediately your manager and IT department. Additionally, employees should be more discreet on social media and limit posts and communications relating to company business. Businesses and organizations can also include the following technical solutions to safeguard against the spreading of malware.

- Perimeter defense such as firewalls are important for preventing unwelcomed entry into systems
    - A perimeter firewall between the onboard network and the internet
    - Network switches between each network segment
    - Internal firewalls between each network segment
    - Virtual Local Area Networks (VLAN) to host separate segments
- Password policy
- Access policies and procedures including two-factor authentication
- Intrusion detection and prevention systems

iii. Cybersecurity Best Practices: Company business network ransomware

Email incidents can occur because company employees are deceived into clicking on links in their email. Some examples of email incidents include phishing and spam emails. In the email example, clicking on a link likely started the ransomware attack. Once the link is clicked, the ransomware can proliferate through the business network; and no longer requires the email system. Phishing attacks can be prevented by the employees before they click on the links. When in doubt, do not click. Some basic cybersecurity best practices to stop the spread of malware are listed below.

- Cyber awareness training: It helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to cybersecurity. Existing company procedures for identifying training requirements should be used to assess the benefits and need for:
    - All company personnel to receive basic cyber awareness training
    - Company personnel, who have been assigned with cybersecurity risk management duties, should receive a type and level of cyber training appropriate to their responsibility and authority
- Regarding contractors and third parties:
    - Should have an updated cyber risk management company policy, which includes training and governance procedures for accessible IT and OT

onboard systems

- The shipowner should query the internal governance of cyber network security, and seek to obtain a cyber risk management assurance when considering future contracts and services

- Effective network segmentation
- Incident detection and prevention

III) Mistaken installation of malware

Malware is installed by seafarer's mistake (e.g. infected USB stick) that consequently interferes with its navigation systems and leads to collision, injury, death etc.

i. P&I and/or FD&D Impact

Crew negligence is explicitly covered under P&I rules. Therefore, if the ship is diverted or collides, runs aground, damages third party property, causes an injury to a person or damage to cargo, etc., a Member's standard P&I insurance will apply in the normal manner and cover the liabilities, expenses and costs that arise in relation to the subject incident.

ii. Cybersecurity Best Practices

Good cyber hygiene should be practiced by everyone. Cyber hygiene is so named because these are practices that everyone should be familiar with and are routine. For example, morning routines include brushing teeth. Good cyber practices include scanning your USBs for viruses. Businesses can develop processes to enable good cyber hygiene in employees as outlined below.

- Develop policies and procedures regarding the use of removable media
- Develop procedures for protection of risks from service providers' removable media before connecting to the vessel's systems
- Prevent the application of software updates by service providers using uncontrolled or infected removable media
- Install removable media blockers on all physically accessible computers and media ports
- Install intrusion detection system to identify unauthorized use of removable media
- Deliver cyber awareness training; helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to cybersecurity. Existing company procedures for identifying training requirements

should be used to assess the benefits and need for:

- All company personnel to receive basic cyber awareness training
- Company personnel, who have been assigned cybersecurity risk management duties, to receive a type and level of cyber training appropriate to their responsibility and authority

IV) Cyber hacking of a dynamic positioning system

An offshore supply vessel (OSV) has had its Class-2 dynamic positioning (DP) system hacked while on station providing services to a fixed jacket offshore production platform (platform A) in the Gulf of Mexico in inclement weather. The vessel loses control of both its DP system and main engine rendering the OSV unable to remain on station or maneuver in any way. The OSV drifts off station and makes contact with another fixed jacket offshore production platform (platform B) in the vicinity resulting in damage to that fixed jacket structure, damage to equipment onboard resulting in a fire onboard the platform. The event injured several seamen aboard the OSV and onboard the platform due to the resulting fire.

i. P&I and/or FD&D Impact

In the instant scenario, the OSV's P&I insurance will cover the liability of the OSV to the third parties who sustain injury, damage or loss as a result of the OSV's contact with the offshore Platform B. Accordingly, the P&I club would cover the damages sustained by Platform B, cargo onboard the OSV, the injury to the persons on board the OSV or Platform B, as well as the costs of rescuing/transferring those persons to safe locations. Additionally, in case of any oil leakage or spillage from the vessel or Platform B (this may happen if it is an oil producing platform) as a result of the vessel's contact with the platform, then P&I insurance would respond to that pollution claim. Here, the P&I claims handler will assess the extent of cover in consideration of the principle that the P&I insurance responds to liabilities that are not covered under the vessel's hull and machinery insurance. Since the standard hull and machinery conditions also provide cover in respect of liability arising out of the striking by the insured vessel of third party property, it is imperative to evaluate the P&I's cover share (i.e., one fourth or four-fourths). Damages to the OSV will be covered by its hull and machinery insurance.

In addition to the above mentioned claims that are covered by P&I, there will be contractual disputes between the shipowner and the Platform A, which chartered the OSV to deliver supplies. In this case, as a result of the casualty, the OSV could not deliver the supplies to Platform A on time. The Club's FD&D team will assist in handling those claims resulting from the OSV's delay/failure to deliver the supplies to Platform A. FD&D insurance provides cover for claims handling assistance and for costs of employing lawyers and experts, as may be necessary to defend (or pursue) such disputes. Accordingly, the costs of defending those claims by Platform A will fall within the vessel's FD&D insurance cover. FD&D cover is by its nature discretionary in that the Club would consider several factors including the merits of the Member's case/defense, quantum of the case, that the expenditure would not be outweighing the aimed beneficial result, and whether the Member acted prudently (i.e., has exercised the standard duty of care) to avoid such incident and resulting delays. FD&D does not cover the principal sum in dispute, such as the cost of delays in the instant scenario.

ii. Cybersecurity Best Practices

Until recent times, DP systems were historically not connected to the administrative networks or the internet aboard vessels. With more highly evolved and automated DP systems being installed on vessels, it is becoming commonplace for these system original equipment manufacturers (OEM) to offer remote diagnostics and maintenance. DP systems, as well as any other control system, are now becoming increasingly more vulnerable to cyber attack due to added connectivity. Additionally, due to the complexity

of the DP system, most vessel owners must rely on the OEM, system vendors, or other third party support personnel to maintain and repair to prevent cases of failure. Therefore, it is imperative to ensure technologies and procedures are in place to properly protect connections, track maintenance activities, and manage onboard OEM, system vendors, or other third party support personnel.

In this example, the threat actor would not require a connection to "hack" the system. A virus could have been introduced during a routine maintenance activity. Crew members could have prevented the hack by reviewing and applying cybersecurity procedures with the support personnel or scanning the USB drives containing DP updates for viruses before plugging into the DP system. In such instances, shipowners may apply both procedural and technical best practices as outlined below.

- Develop policies and procedures regarding the use of removable media
- Develop procedures for protection of risks from service providers' removable media before connecting to the vessel's systems
- Prohibit the application of software updates by service providers using uncontrolled or infected removable media
- Deliver cybersecurity onboarding training to OEM, system vendors, or other 3rd party support personnel
- Perimeter defense such as firewalls are important for preventing unwelcomed entry into systems
    - A perimeter firewall between the DP, onboard network, and the internet
    - Data diodes or the use of one-way (unidirectional) gateways between the DP network and external networks
- Where remote maintenance and diagnostics connections exist
    - Route all external connectivity through a dedicated network or redundant network segments were internal company-controlled security tools are in use to monitor traffic
    - Implement network traffic monitoring and packet scanning

AMERICAN STEAMSHIP OWNERS MUTUAL PROTECTION & INDEMNITY ASSOCIATION, INC.

ABSG CONSULTING, INC.

SHIPOWNERS CLAIMS BUREAU, INC., MANAGER

One Battery Park Plaza, 31st Floor
New York, New York 10004 U.S.A

TEL +1 212 847 4500
FAX +1 212 847 4599
WEB www.american-club.com
EMAIL info@american-club.com

2100 West Loop South, Suite 1525
Houston, TX 77027 U.S.A

TEL +1 346 223 9900
EMAIL claims@american-club.com

SHIPOWNERS CLAIMS BUREAU (UK) LTD.

78-79 Leadenhall Street
London EC3A 3DH, U.K.

TEL +44 20 7709 1390
EMAIL claims@scb-uk.com

SHIPOWNERS CLAIMS BUREAU (HELLAS), INC.

Filellinon 1-3, 3rd Floor
Piraeus 185 36 Greece

TEL +30 210 429 4990
FAX +30 210 429 4187
EMAIL claims@scb-hellas.com

SCB MANAGEMENT CONSULTING SERVICES, LTD.

The Workstation, 28th Floor
43 Lyndhurst Terrace, Central
Hong Kong SAR People's Republic of China
TEL +852 3905 2150
EMAIL hkinfo@scbmcs.com

SCB MANAGEMENT CONSULTING (CHINA) CO., LTD.

Room 905, Cross Tower
No. 318 Fuzhou Road
Shanghai 200001 People's Republic of China

TEL +86 21 3366 5000
FAX +86 21 3366 6100
EMAIL claims@scbmcs.com

1701 City Plaza Drive
Spring, TX 77389 U.S.A.

TEL +1 281 673 2800
FAX +1 281 877 5946
WEB www.abs-group.com
EMAIL info@abs-group.com

ABS Group of Companies, Inc. (www.abs-group.com) provides data-driven risk and reliability solutions, including industrial cybersecurity services, to help clients reduce risk and confirm the safety, integrity, quality and efficiency of their critical assets and operations. Headquartered in Spring, Texas, ABS Group operates with more than 1,000 professionals in over 20 countries serving the marine and offshore, oil, gas and chemical, government and industrial sectors. ABS Group is a subsidiary of ABS, one of the world's leading marine and offshore classification societies.