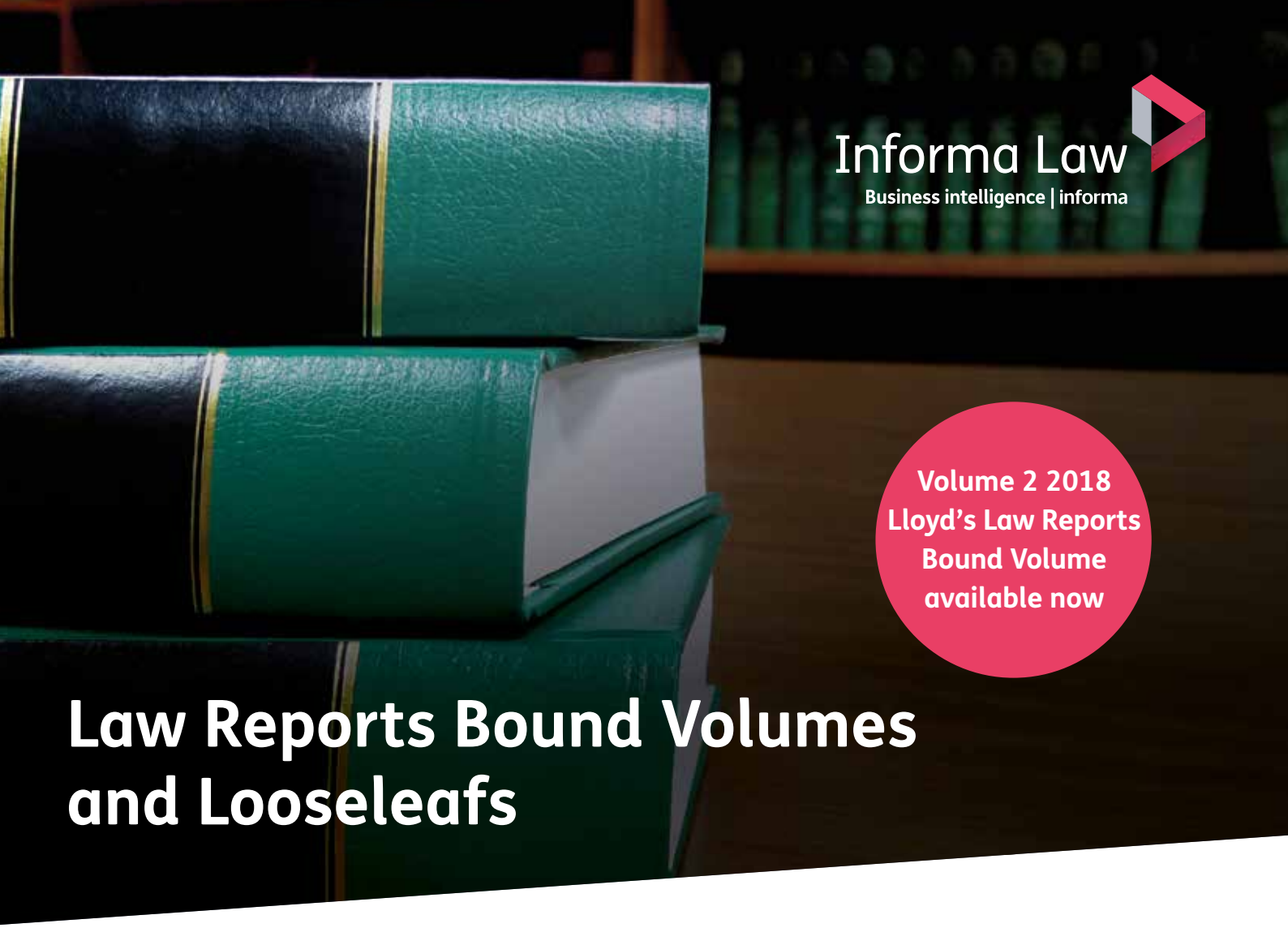
Maritime Risk International
Business intelligence | informa
P&I, claims management and loss prevention
Volume 33 Issue 5 June 2019

Piracy threats

Warning on continuing risks

- Sanctions with an Asian focus analysed
- Safe anchoring flags skills and experience
- Tips to reduce cyber threats



Informa Law
Business intelligence | informa

Volume 2 2018 Lloyd's Law Reports Bound Volume available now

Law Reports Bound Volumes and Looseleafs

Informa Law is a specialist publisher in the field of commercial law. Our Bound Volume collection dates back to 1919 and includes the iconic Lloyd's Law Reports series, as well as bound volumes for our leading review journals.

Bound Volume Series
available as full sets, small bundles and individual units

Make sure your legal library is complete
Each volume contains fully headnoted, verbatim judgments. Each new printed Bound Volume collects the most noteworthy legal decisions reported within the year.

- Access cases and precedents across the full print archive.
- Carefully crafted headnotes crystallise the most significant cases from the world-renowned commercial courts of England and Wales.
- Recent volumes include the most influential cases from overseas jurisdictions.
- Our distinguished editors include high court judges, eminent professors, the Immediate Past Chair of the Bar Council, and leading QCs.

Annual editions of our leading Journals are also available in Bound Volume format.
Lloyd's Maritime and Commercial Law Quarterly
International Construction Law Review

Looseleafs

Our collection of Looseleafs are updated throughout the year and cover all the latest legislative developments in your practice area ensuring you are armed with all the facts and information you need.

- Our looseleafs are the major reference works in the fields of **Insurance Law**, **Arbitration Law** and on the **Ratification of Maritime Conventions**
- Your purchase includes the current edition of the publication, as well as a year's worth of updates.

Contact us today to complete your collection and to receive our special rates.

lawsales@informa.com about.i-law.com +44 20 7017 7565 (EMEA) 65 6508 2428 (APAC)

Informa Law
Business intelligence | informa

Editor: Liz Booth
liz@lizbooth.co.uk

www.i-law.com
www.maritime-risk-intl.com

Maritime Risk International is published by Informa Law, Third Floor, Blue Fin Building, 110 Southwark Street, London SE1 0TA. *Maritime Risk International* provides detailed coverage of legal, technical and insurance issues facing the shipping industry. This ensures you are fully aware of the implications of key court decisions as well as providing in-depth analysis and expert advice on topical issues such as loss prevention, carriage of goods, salvage, ship security, pollution and maritime law. Our maritime content is available online via single-user subscriptions or multi-user licences at https://www.i-law.com/ilaw/maritimelist.htm including our major reference works, *Voyage Charters* (ISBN 978 0415833608) and *Time Charters* (ISBN 978 1843117513).

Client Services: Please contact Client Services on tel: +44 (0)20 7017 7701; +65 65082430 (APAC Singapore), or email clientservices@i-law.com

Editorial queries: Please contact Yvonne Knock, on tel: +44 (0)20 7017 5276, email yvonne.knock@informa.com

Print managed by: Paragon Customer Communications

Registered Office: 5 Howick Place, London SW1P 1WG. Registered in England and Wales No 1072954.

Cover image: US Navy

In this issue

REGULARS

FEATURES

IN BRIEF

Cyber policy

Insurer Beazley has created a marine cyber insurance product to meet the rapidly developing needs of vessel owners and operators. Should a cyber incident impact a vessel's operational capabilities, Beazley Cyber Defence for Marine provides insurance for physical damage and loss of hire. Risk management services are provided, designed to reduce the likelihood of a cyber incident and demonstrate compliance with forthcoming IMO guidelines. There are three risk management elements included: a self-assessment questionnaire; a cyber security workshop; and an onboard cyber survey.

Sustainable shipping

Stena Line has released its third sustainability review "A Sustainable Journey", describing initiatives, improvements and challenges in operations from a sustainability perspective as well as results on their ambitious sustainability targets. The review also highlights the main initiatives of the past year. Stena Line's sustainability strategy is divided into five focus areas tied to the UN Global Goals for sustainable development with ambitious targets set in each focus area. They are equality and inclusion, good health and wellbeing, clean energy, responsible consumption and life below water.

Business buy

Oakley Capital Investments has announced that Oakley Capital IV has partnered with the management teams of SG MidCo AS (Seagull), and Videotel Marine Asia Ltd and Super Dragon Ltd (collectively "Videotel"), to acquire majority stakes in the businesses from their current shareholders, Herkules Private Equity Fund IV and KVH Industries, respectively. For the past 40 years, Videotel and Seagull have established themselves as the best-in-class providers of e-learning to the maritime sector globally and in 2018, the two companies collectively generated US$50 million of revenue. The management teams of Seagull and Videotel believe opportunity can be grasped most effectively by working together as a combined group.

Concern remains for global marine underwriting from attritional losses

While in general, major losses remain stable, the continued erosion of the global premium base means that attritional losses are becoming much more significant. The increased risk of large, more complex and costly claims has the potential to impact all marine underwriting sectors in 2019, according to the International Union of Marine Insurance (IUMI).

Although the global fleet continued to grow at around 3 per cent in 2018, the number of total losses (vessels over 500 gt) stood at a 20-year low. Only 21 total losses were recorded last year and this is on the back of a general downward trend witnessed since 2010. The reduction was seen across all vessel classes. Serious casualties (excluding total losses) have stabilised for the past three years but are still higher, on average, than in 2014. There is likely to be a spike in Q1 2019 when numbers have been finalised. 900 incidents were recorded in 2018 representing 1.6 per cent of the global fleet (or 1.2 per cent in gt).

Looking at cargo insurance, on the back of a slowdown in global economic growth (forecast to reduce from 3.2 per cent in 2018 to 2.8 per cent in 2020), the WTO is expecting growth in global trade to scale back to 3.7 per cent this year (from 3.9 per cent in 2018). As a result, the outlook for shipping is mixed. Container trade is expected to grow by 4.8 per cent in 2019 against a fleet growth of just 2.6 per cent which indicates a modest recovery in rates. However, factors such as a downturn in the economy, increased tariffs and rising fuel costs have the potential to put the brakes on any future upturn.

Dry bulk trades are forecast to grow on average by 3.2 per cent against a fleet growth of 2.7 per cent, which bodes well for a modest uptick in rates this year, albeit from a low base. Conversely, while demand for crude oil is positive, the amount being transported by sea is only expected to grow by 1.4 per cent against a fleet growth of 4.7 per cent. This, together with the current order book and the impact of the impending environmental regulations, makes the outlook for tanker freight rates uncertain.

In terms of cargo losses, nat cat losses in 2018 were lower than in 2017 but were significant nonetheless and included hurricanes Florence, Michael and typhoon Jebi. The fire on *Maersk Honam* in March 2018 is likely to be the largest general average loss in history. Of growing concern is the recent spate of shipboard fires including *Sincerity Ace*, *Yantian Express*, *APL Vancouver*, *ER Kobe* and *Grimaldi Grande America*.

While IUMI cannot speculate on the causes of these fires, past issues such as cargo mis-declaration, improper packing, loading, labelling and shipping of hazardous cargoes are likely to be factors. Other significant issues have included loss of containers overboard, notably the 300 boxes lost from *MSC Zoe* in the North Sea. ***MRI***

Failure to check charterparty wording catches ship manager

The International Transport Intermediaries Club (ITIC) has urged ship brokers and managers to check the terms of their charterparty agreements closely before signing, to avoid costly mistakes further down the line. By way of illustration, ITIC cites the case of the manager of a tanker entering West African waters who believed that the terms of a charterparty provided that armed guards were to be appointed at the charterer's expense. The manager duly appointed the guards for the voyage at a cost of US$170,000, but the charterer refused to pay the invoice.

The terms of the charterparty did in fact include provisions relating to the appointment of armed guards, but their deployment was not mandatory. In addition, the charterparty provided that the charterer was only liable for up to $20,000 of any such costs. The charterer offered to pay that $20,000 and the owner demanded that the managers pay the shortfall.

ITIC says it has seen a number of claims caused by ship brokers and managers acting on their recollection of a charterparty wording, as opposed to checking what the charterparty actually says. On this occasion, ITIC reimbursed the full claim of $150,000. ***MRI***

London has 80 per cent of global maritime arbitration market

Research by law firm HFW has found that London continues to dominate the market for maritime arbitration, despite suggestions that Brexit would see activity shift to emerging disputes hubs around the world. London accounts for more than 80 per cent of global maritime activity, according to HFW's analysis of data from 13 major maritime institutions around the world.

London handled approximately 1,500 maritime arbitrations in 2017, compared to around 140 in Singapore and just over 100 in Hong Kong. HFW's research also found that, after local law, English law is the most commonly chosen law in arbitrations globally across all sectors, including maritime arbitrations. English law was the applicable law in 85 per cent of all LCIA arbitrations in 2017.

Craig Neame, partner, HFW said: "There has been a lot of debate about whether London will lose business as a result of Brexit. Our research clearly shows that, when it comes to shipping disputes, London is still the clear market leader, and we see nothing to suggest that will change in the foreseeable future.

"Singapore and Hong Kong will continue to be attractive to companies operating in Asia, and Dubai and the Nordic countries will develop a larger arbitration caseload once EMAC and NOMA become more established. But English law will remain a popular choice among those in the shipping industry and we expect London to continue to attract the majority of maritime arbitrations." ***MRI***

Lessons learnt from crew injury when securing a tow include better planning

Lessons are to be learned from a recent incident of a crew member being injured when securing a tow, according to David Nichol, senior loss prevention executive at UK P&I Club.

"After completion of loading and with a pilot on board, the forward and aft deck teams were ordered to commence singling up the mooring ropes. The aft mooring team consisted of the second officer in charge, an AB and fitter," he said.

"Once the outboard stern lines were let go and hauled in, instructions were given to make a tug fast through the centre lead. The AB passed a heaving line to the tug crew, who secured the end to a messenger line and gave the signal for the ship to commence heaving in the messenger and tow wire.

"After the slack was pulled in by hand, the messenger was led around two sets of bitts and onto the winch warping drum by the AB. At this time, the second officer was stationed on the starboard aft corner of the poop deck and the fitter was operating the winch controls.

"With four turns on the warping drum, the crew continued to haul in the messenger under power and just as the eye of the towing wire entered the fairlead, the messenger suddenly parted, with one end violently snapping back and striking the AB on the head. The AB sustained a serious eye injury.

"The messenger may have come under excessive strain due to insufficient slack on the wire combined with additional friction created by the eye passing through the fairlead. However, the crew should have been alert to the possibility of the line becoming taut without warning.

"The AB was unsupported at the warping drum, where he was tasked with both handling the rope from the drum and coiling down the slack. On a Panamax bulk carrier, expecting three crew members to safely manage an operation of this nature was probably asking too much."

Lessons learnt included: all mooring and towing operations should be properly risk assessed and planned to ensure all involved crew are aware of how the operation is to be conducted as well as to the potential hazards and safety precautions; mooring crew must be adequately certified, trained, experienced and of a sufficient number to conduct operations safely; and the officer in charge must carefully monitor the tension on lines and give warning where there is risk of them becoming taut. ***MRI***

IN BRIEF

Resilient results

The Shipowners' Club has reported resilient results for the year ending 31 December 2018, with a combined ratio of 104.2 per cent, against the budgeted 105 per cent. Tonnage increased by 6.9 per cent to 27.3 m tonnes and insured vessel numbers increased by 3.5 per cent to 34,094. There was a reduction in capital and free reserves of US$37.9 million, taking net assets to $303.8 million. Chairman Philip Orme said: "The Club anticipated the difficult trading conditions for many of our members and, in the spirit of mutuality, chose to budget for a small underwriting deficit, rather than seek additional premium. It has been pleasing to note that the first quarter of 2019 has seen an upturn in investment markets to the extent that the Club has substantially recovered the 2018 investment deficit."

Business sale

Braemar Shipping Services has announced the proposed disposal of three business lines within the Braemar Technical Services division (offshore, adjusting and marine) to Aqualis ASA in exchange for a significant equity stake in the combined group. Aqualis is a leading provider of consultancy and engineering services to the offshore oil and gas and offshore wind sectors, and is listed on the Oslo Stock Exchange (OSE:AQUA). The combined business will be led by the Aqualis management team, as enhanced by the inclusion of Grant Smith to lead insurance service.

Clean shipping

The Clean Shipping Alliance 2020 (CSA 2020) has received written approvals and no-objection letters from several port authorities around the world indicating they have no intention of banning the use of open-loop scrubbers in their waters. Following successful meetings between port officials and CSA 2020 Executive Committee members, the ports approached indicated that they do not intend to submit any papers to IMO pertaining to exhaust gas cleaning systems operation unless new, compelling research comes to light.

IN BRIEF

New Ukrainian rules

On 27 April 2019 the Resolution of the Cabinet of Ministers of Ukraine "On Certain Issues of Deregulation of Economic Activity" dated 27 March 2019, No 367, was officially published, impacting ballast water regulations. It came into force on 28 April 2019. The Resolution suspended the effect of the provisions, which provided for the inspection of bilge, sewage and ballast water (except for isolated ballast), and amended a number of regulatory acts, which regulated the issue of state supervision (control) over ballast water.

Anti-corruption boost

Britannia has become the first P&I Club to be accepted as a member of the Maritime Anti-Corruption Network (MACN). Established in 2011 by a group of maritime companies committed to eradicating the industry of all forms of corruption, MACN has grown into a global business network of more than 100 members, representing a sizeable percentage of the global fleet. MACN director, Cecilia Müller Torbrand, said: "The effect of maritime corruption is felt across the industry. Britannia's recognition of the problem, and their support for MACN, is an important step in showing a united front against corrupt practices." By joining MACN, Britannia will be able to provide the network with input from an insurance sector perspective.

Skuld positive

Skuld has announced a positive bottom line result of US$11 million ($58 million in 2017) for its 2018 financial year ending 20 February 2019, and a total combined ratio of 98 per cent. Gross earned premium in 2018 amounted to $402 million. The result marks continuity in a record-breaking 16th consecutive year during which Skuld has reported a positive underwriting result. The 2018 year saw challenging conditions in global insurance and investment markets. Skuld experienced a handful of large claims, but overall claims frequency remained low, which contributed positively to the 2018/2019 result. However, a high number of large claims submitted to the International Group of P&I Clubs' joint pool added significantly to 2018/2019 costs.

Africa challenge to realise marine power

African businesses are being challenged to wake up to the economic, social and environmental power of the "Blue Economy". Momentum is gathering for companies based in Africa's coastal nations to fully recognise and understand the benefits of backing a Blue Economy, which covers a wide range of productive sectors that are crucial for the continent's sustainable development, including fisheries, aquaculture, transport, energy, trade and tourism as well as extractive industries.

Research indicates that the Blue Economy has the potential to be a major source of wealth and prosperity for the continent and help advance the African Union's Agenda 2063 and the UN Agenda 2030 for Sustainable Development. The importance of a cohesive strategy to protect and use Africa's coastal waters cannot be overstated, say the organisers of the second Africa Blue Economy Forum (ABEF). It found:

- 70 per cent of Africa's nations are coastal.
- 90 per cent of the continent's imports and exports are transported by sea.
- Africa's maritime industry is estimated to be worth US$1 trillion per year.
- The asset value of ocean economy eco-systems is valued at $24 trillion.
- Plastic pollution costs $13 billion per year due to damage caused to marine ecosystems.

Leila Ben Hassen, organiser and founder of ABEF2019, said: "There needs to be more awareness of the Blue Economy and a realisation of how important it is to the future of Africa. Governments are beginning to understand this and implement policies but it still needs the private sector to grasp this and to look at how it can work in partnership with governments and other organisations to make this succeed. Collaboration is necessary to make this work and deliver huge benefits for the continent enabling it to meet the United Nations' Sustainable Development Goals." ***MRI***

GreenVoyage-2050 launched to support IMO's GHG reduction strategy

A major international project to support the IMO's initial strategy for reducing greenhouse gas (GHG) emissions from shipping has been launched. GreenVoyage-2050 will initiate and promote global efforts to demonstrate and test technical solutions for reducing such emissions, as well as enhancing knowledge and information sharing to support the IMO GHG reduction strategy.

The project is a collaboration between IMO and the government of Norway and will run for an initial two-year period. More than 50 countries in 14 sub-regions are expected to participate, including developed countries and strategic partners from the private sector.

The project will also build capacity in developing countries, including small island developing states and least developed countries. Initially, eight countries, from five high-priority regions (Asia, Africa, Caribbean, Latin America and Pacific), are expected to take pilot roles, to pursue and undertake actions at the national level. These pilot countries will then become "champions", galvanising momentum by supporting other partnering countries in their respective regions to follow a similar path.

IMO secretary-general Kitack Lim thanked the Norwegian government for its financial support for GreenVoyage-2050 – NOK10 million (US$1.1 million) for the initial two years of the project and for the intention to fund the project beyond the two years. He also drew particular attention to the importance of private-sector participation in the project. "I am particularly encouraged by the fact that the GreenVoyage-2050 project is designed with a private-sector partnership component," he said. "This will accelerate the uptake of technology solutions by the industry."

GreenVoyage-2050 will eventually be scaled up with more technology demonstration and infrastructure efforts and with more pilot countries joining the project through mobilising additional resources. Partnerships with existing programmes will also be explored, with a view to drawing on their results to encourage the phasing in of zero and low-emission solutions for shipping in developing countries.

Sveinung Oftedal, specialist director of the Norwegian Ministry of Climate and Environment, said: "By addressing one of the highest priority environmental issues faced by maritime transport sector and by catalysing development of technological solutions, GreenVoyage-2050 can substantially contribute to the UN sustainable development goals and the objectives of blue economic growth in developing regions". ***MRI***

BIMCO

NEW PRESIDENT

Şadan Kaptanoğlu, managing director of HI Kaptanoğlu Shipping, has been elected president of BIMCO at its general meeting in Athens.

Şadan, who is a Turkish shipowner, takes over from Greek shipowner, Anastasios Papagiannopoulos, Principal of Common Progress, who has completed his two-year term as president. Sadan takes over after a two-year period as president designate and will be the first female president of BIMCO.

Sabrina Chao of Wah Kwong in Hong Kong was elected as president designate and joins the board of directors.

Baltic Exchange Council

NEW CHAIRMAN

Denis Petropoulos has been elected chairman of the Baltic Exchange Council. He replaces Duncan Dunn who has held the position since January 2018. Denis was a founding partner of Braemar Tankers Ltd and remains a significant shareholder at Braemar Shipping Services plc. He recently headed up Braemar's Singapore office for seven years, before returning to the UK.

He has been a Baltic Exchange member since 1999 and has held positions on the Baltic board from 2002 to 2007. He joined the Council in January 2019.

Denis has worked in competitive ship broking for 40 years. He presently sits on INTERTANKO's associate members' committee and is a non-executive director of TEN, a New York Stock Exchange-listed tanker company.

Denis left H Clarksons in 1985 to open Braemar Tankers, which by 2001 was a publicly listed company where he sat on the board. In 2011 he opened the group's shipbroking office in Singapore and remained there until 2017 heading up the corporation's expanding operations in the Asia-Australia region. He came off the plc board in 2015 and is now based in London.

Trinity House

RETIREMENT

Edgar King has retired after 24 years as event manager for Trinity House, the working home of the General Lighthouse Authority. Previously deputy events manager for the past 12 years, Zoe Turner will become the newly titled role of head of events and Natasha Jackson has been appointed senior events manager.

Wallem Group

NEW MANAGING DIRECTOR

John-Kaare Aune has been appointed the new managing director, Ship Management, for the Wallem Group. He is expected to take up his position with effect from 1 July 2019.

John joins Wallem from the Cayman Registry, where he was most recently regional director, safety and compliance, overseeing its global commercial services and business development in addition to the registration section in the Asia-Pacific region. Previously John served as principal surveyor with the Cayman Registry.

John is a qualified naval architect and spent more than six years with the Norwegian Maritime Directorate (NMD). During this time, he represented Norway on numerous EU expert committees and several different IMO Committees. John has also served as the executive secretary to the Cayman Islands Shipowners Advisory Council. He has played a key role in the growth of the Cayman Registry and in maintaining its established position on the Paris and Tokyo MOU white lists.

LOC Group

NEW TECHNICAL DIRECTOR

LOC Group has appointed Paul Walton as the technical director of shipping for the London office. Paul is returning to LOC London after serving as a director of the group's Hong Kong office. Paul has been with LOC for eight years, joining the group in 2010 as a master mariner.

Paul is a Class 1 master mariner with 18 years' seagoing service on container ships, bulk carriers, general cargo vessels, and heavy lift vessels. Paul spent five years coordinating on-shore container stowage and the following 13 years in ship management for tankers, bulk carriers and offshore vessel fleets.

Previously, Paul led the group's Hong Kong office, undertaking investigations into various types of marine casualties, specialising in collisions, groundings and bulk cargoes.

UK P&I Club

NETHERLANDS SUBSIDIARY

The UK P&I Club has won approval from the Netherland's financial regulator for a licence for its Rotterdam-based subsidiary, UK P&I Club NV.

The UKNV Rotterdam office is located in the World Port Center and the management board based in Rotterdam consists of: Hugo Wynn-Williams as chief executive officer; Paul van den Brom as chief financial officer; and Rene Doff as chief risk officer.

Brookes Bell

NEW SCIENTISTS

Brookes Bell has appointed four PhD-level cargo scientists to its UK and Asian teams.

Brookes Bell's cargo scientists provide expert opinion, as well as assisting in determining the cause, nature and extent of spoilage and contamination incidents involving cargoes such as grains and animal feeds, chemicals, fertilisers, liquefaction of minerals, self-heating and fires.

Brian Ward and Marcelo Rodrigues have joined the Brookes Bell UK Science team, based in Liverpool, and will report to Martin Jonas, head of cargo science UK. Karwei So and Wen Li have joined the Brookes Bell Asian team, based in Hong Kong and Shanghai respectively, reporting to Tim Moss, head of cargo science Asia.

Meanwhile, the company was nominated in two catergories in the recent Mersey maritime Awards 2019, for business of the year and maritime professional services award.

Synergy Group

WINS AWARD

The Synergy Group's commitments to safety at sea, seafarer welfare and female empowerment in the maritime workforce were recognised at the 2019 Seatrade Awards in London. The Singapore-based shipmanager won the prestigious 2019 Seatrade Award for Investment in People. The award identifies "a significant contribution to the recruitment, training, retention and advancement of the industry's most valuable asset – its people".

Chalos & Co

RECOGNITION

Michael Chalos, of Chalos & Co, has been recognised by Chambers USA as a leading practitioner in the field of shipping and maritime litigation. Michael was listed among 15 lawyers in the field nationwide.

Shipping faces new Gulf risks

Targeted attacks on four ships off the UAE have raised concerns about the security of shipping in the region and sparked an extraordinary meeting of the war risks committee at Lloyd's

Lloyd's of London insurance market has widened its list of areas in and around the Gulf posing "enhanced risk for marine insurers" after attacks on ships off the United Arab Emirates (UAE).

Lloyd's said that the Gulf, part of the Gulf of Oman, Oman and the UAE had been added to the list. Saudi Arabia's risk areas were meanwhile expanded to include its coasts.

It comes after marine insurers in London held an extraordinary meeting to discuss the situation in the Gulf.

The meeting was of the Lloyd's Market Association (LMA) Joint War Committee (JWC) which normally gathers on a quarterly basis to assess security risks to shipping around the world.

"The London insurance market's JWC has been considering developments in the Gulf," said Neil Roberts, head of marine and aviation at the LMA, which represents all underwriting businesses on the Lloyd's of London insurance market.

"In the light of further information received, the JWC has issued this advisory notice to the market, amending the listed areas which detail areas of perceived enhanced risk for marine insurers and reflecting the enhanced regional risk," he added in a statement.

It follows insurgent drone strikes on a key oil pipeline in Saudi Arabia and the mysterious sabotage of four ships, including two Saudi oil tankers, in May.

The ship attacks have escalated tensions between the US and Iran but industry analysts have questioned the circumstances surrounding them.

Lloyd's List Intelligence, Informa's business information service, said there had been "scant information" about the incident from Saudi authorities.

"Saudi reticence to report the incident accurately within its own media channels and the current failure to provide imagery evidence of the attack raises important questions as to the nature of the attack," maritime security company Dryad Global told clients in a note, *Lloyd's List* said.

Attacks on Saudi and UAE oil assets built to bypass the Strait of Hormuz, a strategically important waterway in the Gulf, have raised fears that alternative routes could be vulnerable.

Four ships including two Saudi oil tankers were damaged in mysterious sabotage attacks off Fujairah, an emirate located at the crucial entrance to the Gulf. That incident was followed by drone strikes by Yemen's Huthi rebels on a major Saudi oil pipeline, which provided an alternative export route if the Strait of Hormuz closed.

Areas already on the centuries-old insurance market's JWC Hull War, Piracy, Terrorism and Related Perils list include Israel, Libya, Pakistan and Venezuela.

ASSOCIATED PRESS

Meanwhile, Naval Dome CEO, Itai Sela, said: "It is deeply worrying that four tankers have been attacked outside the strategically important Strait of Hormuz. Our indications are that these incidents could develop to include cyber attacks on vessels operating in the region.

"It is highly likely that vessels operating in high-risk areas could be targeted, systems hacked and GPS spoofed to render vessels immobile or re-directed as part of wider actions. There has been increased activity in the cyber domain over the last few months, which is very worrying.

"While we hope these incidents will not escalate, shipowners with operations in the area must be vigilant and carry out inspections of all their PC-based navigation and machinery control systems. Ship operators should not allow crew members or technicians to plug-in USBs or external devices onboard or download maps and charts for specific areas, unless they absolutely need to do so. We also advise that operators check their insurance policies to ensure that OT systems are covered in the event of any cyber damage."

The attacks

Jake Longworth, senior intelligence analyst at security firm EOS Risk Group, provides further commentary on the attacks below.

Each vessel has a 5 to 10 ft hole in its hull, caused by an explosive charge detonated below the waterline. There were no reported spillages and no reported disruptions to port operations or bunkering at Fujairah. The targeted vessels were *Al Marzoqah*, *Amjad*, *Andrea Victory* and *A Michel*.

What caused the damage?

A team of UAE and US military experts are assessing the victim vessels and there is still no definitive explanation as to what caused the damage. However, there is general agreement that

the ruptured hulls were caused by explosive charges/munitions detonated below the waterline. Most experts and analysts believe the explosives were delivered by either underwater divers (ie attaching limpet-style mines) or remote/GPS-controlled underwater drones.

Who was responsible?

At this stage, the finger is widely being pointed at Iran (the Islamic Revolutionary Guards Corp Navy (IRGCN)) or its proxies. After all, Tehran has become increasingly agitated over the expansion of US sanctions and US withdrawal from the Joint Comprehensive Plan of Action (JCPOA). For years, Iran has regularly threatened the US and its allies by saying it could close the Strait of Hormuz or launch devastating attacks in the Gulf region.

In April 2019 the head of IRGCN stated: "If we are prevented from using it, we will close it ... In the event of any threats, we will not have the slightest hesitation to protect and defend Iran's waterways." In July 2018 the IRGC commander said: "We will make sure the enemy understand that either everyone can use the Strait of Hormuz, or no one." In the same month, Iranian president Hassan Rouhani, while discussing the prospect of Iranian oil exports being halted, threatened: "If you can do such a thing, do it and see what happens."

Past bouts of Iranian sabre rattling have been nothing more than that, but in the week running up to the incidents at Fujairah, the US sent additional forces to the Gulf region amid escalating tensions with Tehran. Forces and equipment included the *USS Abraham Lincoln* carrier strike group, a US Air Force B-52 bomber task force, *USS Arlington* and a Patriot missile defence battery. The Pentagon said that US forces were responding to a "credible threat by Iranian regime forces" but did not offer any specifics. In response to the military deployments, Iran accused the US of conducting "psychological warfare".

In addition, the US Maritime Administration (MARAD) warned US-flagged vessels that: "Since early May, there is an increased possibility that Iran and/or its regional proxies could take action against US and partner interests, including oil production infrastructure, after recently threatening to close the Strait of Hormuz. Iran or its proxies could respond by targeting commercial vessels, including oil tankers, or US military vessels in the Red Sea, Bab-el-Mandeb Strait, or the Persian Gulf."

ASSOCIATED PRESS

Iran has denied any involvement in the attacks. On 13 May, Iranian foreign Ministry spokesperson Seyyed Abbas Mousavi said the incidents were "alarming and regrettable", but that more details were needed. Indeed, a more sinister conspiracy is that an anti-Iranian entity played a role in the sabotage to frame Iran, prompting tighter international pressure, additional sanctions and even military retaliation.

Terrorist groups (ie AQAP (Al-Qaeda in the Arabian Peninsula)/ Islamic State) have also been considered as potential perpetrators, although it seems extremely unlikely that such groups would have the means and technology to coordinate such an attack. Furthermore, there have been no claims of responsibility.

Will there be further attacks?

EOS believes that these incidents likely constituted a "one-off strike" designed to deliver a statement, making further attacks in the immediate term (one month) unlikely. If Iran was behind the attacks, it will understand that any additional action is likely to prompt US-allied military retaliation, which, for all Tehran's aggressive rhetoric, is not in its best interests. That said, uncertainty over the identity of the threat source inhibits a well-informed assessment.

If the current level of tension between the US, its allies and Iran persists or increases, further attacks in the broader Gulf region, and in the Red Sea off Yemen, are a credible risk in the medium to long-term, with commercial shipping remaining vulnerable (ie retaliation for oil/tanker sanctions). This risk is likely to mainly impact tankers, especially those with US, Saudi, UAE or allied associations. Broader threats could also spiral in the event of a US-allied strike on Iran. Some analysts do believe that the US is angling itself for war and that the smallest accident or misjudgement could see conflict ignite.

What can be done?

In an Advisory issued 13 May, the Norwegian Maritime Authority temporarily requested that Norway-flagged vessels off Fujairah implement measures equivalent to MarSec Level 2. Other flag states may have issued similar advisories and advice. Following the attacks, vessels operating off Fujairah and in the broader Gulf region are advised to remain at a heightened state of alert.

For a brief time in April to May 2015, the US Navy began escorting US and UK-flagged vessels through the Strait of Hormuz following the Iranian harassment and/or detention of three commercial vessels (*Alpine Eternity, Maersk Tigris* and *Maersk Kensington*). It is unclear whether similar measures will be considered given recent developments.

Unfortunately, the political forces at play and the technicality of such attacks leaves the situation largely outside of the shipping industry's control. Responsibility will predominantly fall to masters to ensure vigilance in the region and to shipping companies to consider potential "vulnerabilities" in their fleets and trading patterns. ***MRI***

Keeping a watching brief: sanctions

Ben Chandler, of The Standard Club, reviews the impact of sanctions on the maritime world, with an Asian focus

In the past two years, the use of international economic sanctions has returned to the forefront of international relations and the global geopolitical landscape. Driving this trend has been the United States' return to an aggressive foreign policy during the presidency of Donald Trump. This has involved the re-imposition of sanctions previously lifted in countries such as Iran, Myanmar and Cambodia; and targeting new sanctions at countries deemed hostile to the Trump administration.

The United Nations (UN) and European Union (EU) have also continued with their own sanctions programmes.

Effect on shipowners/marine insurers

The renewed vigour in the use of sanctions has created additional pressures and burdens on both shipowners and marine insurers. Shipowners have needed to take steps to keep up to date on the changing sanctions landscape and carry out enhanced commercial due diligence to ensure that no commercial activity being undertaken involves a designated sanctioned entity or otherwise breaches sanctions. Similarly, marine insurance providers must be vigilant to international sanctions in relation to their clients' activities. This article focuses on how current trends particularly affect the Asian market.

Sanctions regimes

There are two main sanctions regimes that are most likely to affect shipowners/marine insurers operating in Asia.

UNSC sanctions

Through its resolutions, the UNSC (United Nations Security Council) imposes prohibitions on activities or transactions relating to specified sanctioned countries or individuals. These sanctions are in turn implemented by UN member states through local legislation. Where such legislation is in place, a person who breaches the UNSC sanctions will be liable to criminal penalties. As an example, UNSC sanctions are implemented in Singapore through regulations enacted under the UN Act and MAS Act. Breaches of the UNSC sanctions under Singapore law can result in fines of up to US$1 million and imprisonment of up to 10 years.

US sanctions

Unlike UNSC sanctions, US sanctions are *not* implemented through local legislation and they largely remain targeted at US persons and persons within the US apart from certain US sanctions regimes which also target non-US persons, eg Iran. Non-US persons operating in Asia may also be exposed to the risk of violating US sanctions where:

- They are found to have assisted a US person in evading US sanctions.
- The individuals involved were present in the US when the US sanctioned transaction took place – in which case the individuals will be treated as US persons.
- They are involved in sanctioned transactions which have US connections – for example, where payments are to be made in US dollars, or where US insurers, banks or other US persons or entities are involved.
- They are involved in the re-export of US goods or technology to countries subject to US sanctions.
- They are involved in a transaction that is in breach of US "secondary sanctions" which are targeted against non-US persons.

In addition, a non-US person may find itself "blacklisted" by the US where it continues to do business with US sanctioned entities.

Sanctions imposed by other countries

The US is not the only country that independently imposes "stand-alone" sanctions against other countries or individuals. Examples of such sanctions include those imposed by UAE against Qatar and Russia's sanctions against Turkey. Hence, when carrying out commercial due diligence, shipowners and marine insurers must be alert to all relevant sanctions regimes that may apply.

Examples of recent sanctions developments with respect to specific countries in Asia

Iran

By ending its participation in the Joint Comprehensive Plan of Action (JCPOA), the US has broken ranks with the EU and major economies including China and Russia, which remain parties to the JCPOA. As of 4 November 2018 the US re-imposed sanctions on a range of Iran-related transactions.

The new US sanctions serve to significantly increase the risk of violations by shipping companies involved in shipping Iranian cargo. The restrictions placed on insurance cover also means that Iranian vessels are at risk of having insufficient liability cover in the event of a casualty.

In response to the US sanctions, the EU has implemented "blocking regulations" that seek to counteract its effects. However, these "blocking regulations" only affect EU persons so are likely to have little impact in Asia, unless, potentially, a person or entity primarily domiciled in Asia has a sufficient nexus/connection with the EU so that they are subject to EU law.

North Korea

US sanctions

In March 2018 the US Treasury Department of the Office of Foreign Assets Control (OFAC) amended and reissued North Korean sanctions regulations. The regulations now provide:

- Property of US persons is blocked/frozen in the US if such US persons engage in significant importation from or exportation to North Korea of any goods, services, or technology.
- Foreign financial institutions are prohibited from engaging in most North Korea-related transactions that transit the US financial system.

- Due to the "180 rule" included in the regulations, any ship which calls at a North Korean port or engaged in a ship-to-ship transfer with a vessel that has called at a North Korean port is barred from US ports for 180 days.

UNSC sanctions

In August 2017 the UNSC voted to impose new sanctions against North Korea. Resolution 2371 further expanded the sanctions against North Korea by:

- Prohibiting North Korea from exporting coal, iron ore, lead ore and seafood;
- Prohibiting designated vessels engaging in prohibited activities and from calling at ports of UN member states;
- Prohibiting chartering of North Korean vessels; and
- Extending the list of entities and individuals subject to travel bans and asset freezes.

Fronting

There have been regular occurrences of companies in Asia "fronting" for North Korean entities which are sanctioned. These companies hold themselves out as buyers of cargo from international suppliers and complete ostensibly legitimate trades, but then supply the cargo to North Korean entities in breach of sanctions, for example through ship-to-ship transfers at sea.

Given that such North Korean-linked trades may also include non-North Korean entities and/or ships, and "fronting" activity may be taking place, shipowners/marine insurers must be particularly vigilant when carrying out commercial due diligence, to ensure that the trade does not breach sanctions. Given that much of the "fronting" activity takes place at "hotspots" in eastern Asia, this trend arguably represents an enhanced sanctions risk for Asian shipowners/marine insurers.

Myanmar/Cambodia

Both the US and EU have recently announced fresh sanctions against Cambodia and Myanmar currently taking the form of asset freezes and travel bans on designated person/entities in those countries.

Marine insurance providers and international economic sanctions

In response to the current sanctions climate, marine insurers (including those based in Asia) use a variety of strategies to handle and minimise sanctions-related risk.

Enhanced KYC and due diligence procedures

Marine insurers must have robust "know your client" (KYC) procedures to ensure that no new insurance business involves insuring a sanctioned entity, and that any commercial activity arising from this business does not involve a sanctionable element.

Exclusions to cover

Marine insurers include provisions in their policies/rules which:

- Exclude coverage of an insured loss or claim if it arises from sanctionable activity; and
- Include termination/cessation of insurance provisions which terminate cover for an insured ship if the ship has engaged in sanctionable activity and/or if the provision of insurance to that ship exposes the insurer to sanctions.

Such provisions allow insurers to minimise sanctions exposure and ensure that the insurer does not engage in sanctionable activity as described above.

Sanctions guidance to clients/members

Marine insurers now place an increased emphasis on providing guidance to their assureds on potential sanctions risks. The Standard Club has a 20-person strong sanctions team which includes representatives from both the club's headquarter office in London and each international office. From the Asian perspective, several members of the club's Singapore office are involved in handling sanctions related issues on a regular basis, in conjunction with the Club's international sanctions and compliance teams.

"Shipowners and marine insurers need to continue to monitor the evolving sanctions climate closely and continue to develop strategies to respond to new and existing sanctions risks"

The sanctions guidance has evolved to become a key part of Club service and Clubs will often act as an early point of contact for a member to discuss a sanctions issue, before the matter is then elevated to external sanctions experts as necessary.

Furthermore, many Clubs now place considerable emphasis on regularly producing sanctions-themed guidance materials (eg update bulletins and circulars), which are available free of charge from the Clubs' websites and which are designed to provide user-friendly guidance to the Clubs' members.

Industry consultation/collaboration

As well as providing guidance to their own clients/members, marine insurers are also involved in broader consultation and collaboration across the industry, which The Standard Club is actively involved in.

The future

The use of international economic sanctions is closely linked to the evolving foreign policy outlooks of the US, EU and UN, as well as other states using such sanctions as a political strategic tool. Shipowners and marine insurers will need to continue to monitor the evolving sanctions climate closely and continue to develop strategies to respond to new and existing sanctions risks.

- *The author would like to thank Karnan Thirupathy and Andrew Cook of Kennedys Legal Solutions in Singapore for their helpful input and guidance.* ***MRI***

Ben Chandler

Ben Chandler, senior claims executive, The Standard Club

Fighting the maritime menace

Nazery Khalid, maritime analyst, brings to attention the ever-present threat of piracy and the need for maritime stakeholders to remain vigilant and to strengthen cooperation to reduce its threat

Piracy is a scourge at sea that has haunted sailors since time immemorial. It has continued to be a bother to merchant vessels to this day, with pirates becoming more sophisticated in their approaches and attacks becoming more violent and even deadly.

When one considers that 95 per cent of the world's trade by volume is carried by seaborne means, and how dependent many nations and the global economy are on trade to power their growth, one can immediately put into perspective the significance of the threat that piracy poses to international trade and the economy.

Modern-day buccaneers not only board vessels to steal cargos and the ships and rob crew members of their valuables, they also go as far as kidnapping seafarers for ransom and even injure and kill them after resistance or when the demand for money to secure their release is not met.

The threat of being attacked and kidnapped adds to an already challenging profession for seafarers. The threat posed by pirates is so clear, present and real that marine insurance underwriters insist on cargo owners and shipowners taking up marine kidnap for ransom and hijack (K&R) coverage and charge an additional premium on ships traversing piracy-prone waterways. This is needed as K&R incidents pose threats which may not be covered by normal insurance when crew, cargo and ships are detained. K&R coverage is crucial, not only for the protection of the safety and lives of the crew but also for shipping companies against the ensuing financial costs related to resolving piracy cases. Such costs include paying ransom to release their crew and ships, in-transit loss of ransom money, legal liability cost, consultation fees and payment for death to next of kin and for the treatment of injury and rehabilitation of hostages.

International maritime bodies such as the IMO and shipping associations/NGOs such as International Chamber of Shipping, World Shipping Council, BIMCO, Intercargo and Intertanko are united in their condemnation of piracy as a threat to not only world shipping but also world trade. Governments of coastal states have responded to their concern raised by these bodies about the piracy menace by boosting the resources of maritime security agencies such as coastguards and marine police. More resources and attention have resulted in increased patrols and surveillance and intergovernmental cooperation to share intelligence and conduct joint anti-piracy initiatives. High-risk areas such as the Gulf of Aden and the waters off the Horn of Africa have seen multilateral efforts among navies of several countries engaging in anti-piracy measures to weed out attacks by gangs of pirates which were once roaming rampantly in this critical seaborne trade passage and preying on the many ships traversing there.

Underscoring how seriously it views the piracy threat, the IMO has introduced a set of recommendations to governments and a series of best management practices (BMP) – now into its fourth version – as a guidance for shipowners, ship operators, ship masters and crew to prevent and suppress acts of piracy and armed robbery against ships. The Maritime Safety Committee of the IMO has also issued guidance to shipowners/operators for the use of private armed guards on ships sailing in high-risk areas and has provided recommendations to flag states on the use of such guards.

Such guidelines are most helpful given that pirates are also stepping up their game and continuously changing tactics and methods in mounting attacks. They no longer just use small boats or skiffs with low-powered engines in small teams of two or three attackers to attack small vessels. Somali pirates operating in the northern Arabian Sea off the Indian coast are known to use hijacked merchant ships as "mother ships" as offshore stages to carry out attacks. This is a distance of more than 1,500 nautical miles from the coast of Somalia which presents a telling sign of how increasingly sophisticated and bold they have grown.

Perilous waters

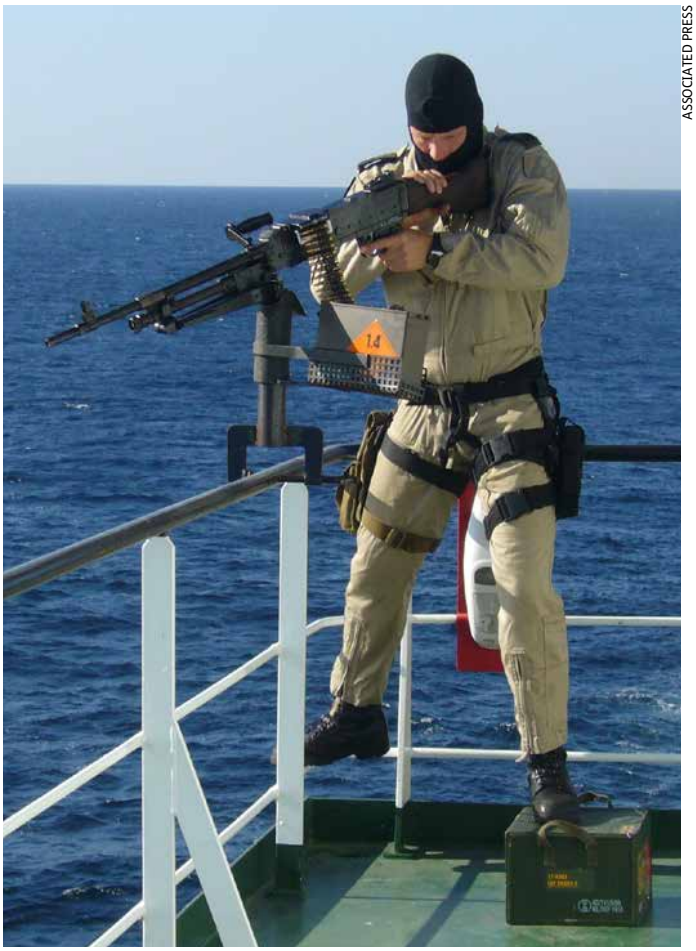
Although the number of pirate attacks on merchant ships has declined in the last few years, there are still a good number of piracy incidents in key waterways that demand stakeholders in seaborne transport and maritime supply chain remain vigilant.

While the presence of international naval and military forces in the Gulf of Aden has helped to quell piracy in this critical waterway, it is still not totally cleansed of the threat. Gangs of pirates from Somalia have continued to mount attacks on vessels transiting the Arabian Sea and the northern part of the Indian Ocean, away from the International Recommended Transit Corridor established by the international task force against piracy in the Gulf of Aden.

Another high-risk area for piracy is the Strait of Singapore south of the Straits of Malacca, the world's busiest and most important trade sea lane. The Strait of Singapore is a busy seaborne passageway leading to Singapore Port, the world's largest transhipment and bunkering port, which handles some of the world's biggest merchant vessels.

Despite efforts by maritime security agencies of the littoral states of the Strait of Singapore to patrol the area, pirate attacks on merchant ships transiting the sealane have continued. Between January and April 2019, the Regional Cooperation Agreement on Combating Piracy and Armed Robbery Against Ships in Asia (ReCAAP), the Singapore-based piracy watchdog, recorded four incidents of "unauthorised boarding of ships" in the western sector of the Strait. These incidents involved tugboats, towing barges and a dredger which were sailing westbound of the Traffic Separation Scheme lane in the Strait. Although no crew was harmed, two of the incidents involved the theft of scrap metal which was transported by barges.

Underscoring the danger faced by ships sailing through this key global trade waterway, ReCAAP has issued a reminder to ship crews to exercise vigilance and adopt extra precautionary measures when in transit there. They are also urged to report all incidents immediately to the authorities of the nearest coastal



ASSOCIATED PRESS

state. ReCAAP has also called on the littoral states of the Strait to increase surveillance and patrols in the busy waterway and respond quickly to incidents reported by ships under attack there.

Governments to the fore

It should now be clear that to completely eradicate the threat of piracy is not an easy task – if not altogether impossible. Piracy presents a complex challenge for all stakeholders in the maritime sector which include governments and their security agencies, industries, businesses, cargo shippers and receivers, marine insurance underwriters, shipowners, ship operators and even coastal communities.

The most difficult aspect to address is the factors on land that result in people taking up piracy as a source of income. Almost always, pirates come from areas which are politically unstable and economically depressed, and from nations often described as "failed states". This provides fertile ground for the recruitment of pirates among people who are frustrated with the lack of work and who look for an easy way out to earn money. Addressing the socio-economic and geopolitical root cause of piracy and the law enforcement vacuum in which it thrives presents the most challenging aspect in the war against piracy.

In this regard, the role of governments in eradicating piracy is pivotal. They bear the biggest responsibility to create a conducive environment in which the rule of law is adhered to. It is just as important for governments to put in place infrastructures such as communications systems and networks and to provide enforcement agencies with the necessary assets and trained personnel to deal with piracy. Given that pirates are upping their game with fast boats operated out of mother ships and are armed with deadly weapons, security agencies need to be able to match the perpetrators. Governments must also ensure that there are laws that can bring the pirates to book and mete out harsh penalties befitting their crime. They also need to prevent, criminalise and prosecute those behind financing and planning piracy attacks, and those involved in recruiting pirates, arming them and acting as facilitators or accessories to their activities.

As piracy is a trans-boundary crime, there is a need for counter-piracy measures to be undertaken on a multilateral platform. It is crucial that governments cooperate closely in areas such as intelligence exchange, patrolling, arrest and prosecution to thwart pirates.

Fighting the good fight

While there are sure signs that piracy is no longer a serious threat in major sealanes such as the Straits of Malacca and Gulf of Aden, thanks to unilateral and international counter-piracy measures undertaken by governments, the threat of pirate attacks on merchant ships still persists. Incidents recorded in waters beyond where the international task forces on piracy operate, for example in southern African waters, and in the Strait of Singapore, show that shipowners/operators, seafarers and governments should not be complacent and must continue to remain vigilant to fight the threat posed by pirates.

Piracy is a threat that warrants serious attention from maritime trade stakeholders, given the importance of shipping to the global economy. Adequate resources must therefore be allocated and provided to protect shipping lanes from pirates who can cause serious disruption to seaborne transport and other maritime economic activities. There has to be strong political will and cooperation amongst governments, maritime security agencies, owners, shipping industry players and other stakeholders in the maritime supply chain to invest in anti-piracy infrastructures and measures, share information and jointly take decisive actions to fight this bane to shipping and also to confront its root causes onshore.

Repercussions such as disrupted supply chains, increased cost of marine insurance and damage caused to ships and cargos have trickling impacts to governments, industries and businesses and also hit the pockets of consumers. As such, the fight against this scourge at sea must continue to be pursued relentlessly by all maritime stakeholders, individually and collectively. They must send a strong message to pirates that their crimes will not go unpunished and will be met by the international community with a swift, harsh response.

- *This is an extract of the full article, which is available online at www.maritime-risk-intl.com* **MRI**

Nazery Khalid

Nazery Khalid, a maritime analyst based in Kuala Lumpur

Ship security integrity hardened

Elena Stefopoulou, of Prevention at Sea, discusses the ways in which vessels can be hardened to withstand an attack by pirates

Recently published 2018 statistics on piracy and robbery against ships show a significant increase of such incidents across the world's seas, especially on the west African coastline. These alarming numbers reinforce the need to fortify vessels by adopting passive (deterrence) and active (defence) ship security measures.

To combat ship piracy, maritime organisations continue to develop new regulations and guidelines aimed at safeguarding seafarers, vessels and their cargo. Let us not ignore the fact that vulnerability of a vessel to an attack by pirates varies depending on type and size of vessel as well as the route taken; therefore, set guidelines are without any doubt key ingredients in preventing piracy attacks. Making them vessel-specific is the cherry on the cake. All anti-piracy measures taken need to be properly thought through and then implemented onboard with a view to protect the crew, the vessel and the cargo in the event of a piracy attack.

On 25 July 2018 the Oil Companies International Marine Forum (OCIMF) issued the publication "Guidelines to Harden Vessels" with a view to provide a layered defence methodology based on lessons learnt from developing best management practices to deter piracy and enhance maritime security. These guidelines can be used as additional guidance to the vessel for specific situations and/or identified threats always in conjunction with the approved ship security plan (SSP) which is the main guidance for each vessel.

In accordance with TMSA (Tanker Management and Self Assessment) element 13.2.1, VIQ7 items 7.8, 7.9, 7.10 and the recently published BMP5 Best Management Practices to deter piracy and enhance maritime security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea, a vessel's hardening plan (VHP) is required to be available and easily accessible onboard vessels.

During the development process of a VHP, other than considering all related regulatory requirements, it is ensured that the plan is not generic but ship-specific by including for example an equipment list related to ship protection measures as well as drawings and extracts from the vessel's general arrangement plan, thus ensuring that hardening positions and points are properly indicated for easy reference by the vessel's crew.

The VHP is not required to include guidance on general navigation practices or on implementation of the International Ship and Port Facility Security (ISPS) Code. Vessel hardening relates to all the physical measures taken to improve the vessel's security integrity. Moreover, any vessel-hardening measures adopted should not compromise in any way the vessel's compliance with the International Convention for the Safety of Life at Sea (SOLAS) regulations; for example, nothing should interfere with the crew's ability to respond to non-security-related emergencies.

It is recommended that additional security training should be provided to the crew in respect to the use of security equipment, hardening points and specific ship protection measures, in accordance to the procedures and measures listed in the ship–specific hardening plan.

Threat detection

OCIMF states that security threats are broadly divided into two categories these being *physical* threats and *virtual* threats. The former can originate from the air, land or sea, whereas virtual security threats come in the form of cyber attacks on electronic hardware and software targeting to disable the vessel's operating systems. Virtual threats cannot be easily identified, as opposed to physical threats.

OCIMF recently released a three-layered defence approach for vessel hardening to assist with how the vessel can control and prevent unauthorised access onboard.

The primary layer prevents unauthorised access to the vessel and at the same time controls access to a vessel. Preventing access while at sea or offshore can be performed using physical barriers for preventing boarding by ladders and grappling hooks. These barriers may include razor wire, GRP spikes, plastic barriers, water and foam cannon systems, guards etc. This layer of defence also enables the vessel to effectively manage unauthorised access while in port or at anchor.

In the event of breach of the primary layer of defence, a second layer of defence enables the crew to prevent or delay intruders accessing the accommodation block, stores and machinery spaces. This layer includes, among other measures, placement of secondary doors outside or inside access points to the accommodation block, a monitoring system with alarms on all doors, and hinged plates on hatches, vents and staircases to obstruct entrance.

If both primary and secondary layers of defence fail, this means that unauthorised intruders now have free access to the accommodation and bridge deck. The third layer of defence is the last bastion against intruders, preventing or delaying them from accessing the vessel's citadel with the use of smoke cannons, strobe lights and noise makers fitted in compartments and alleyways, as well as isolating lift shafts.

Vessel control and safety

Nowadays, intruders are technically capable and know very well how to disable vessel systems such as the automatic identification system (AIS) and the long-range identification and tracking (LRIT) system. For this reason, it is essential for the vessel to regularly report its position to regional authorities.

Standard X-band radar sets may sometimes fail to pick up small vessels, especially if their hulls are made of glass, reinforced plastic or wood. The ship operator needs to come up with innovative solutions aiming at installing new equipment or upgrade existing vessel systems to ensure efficient ship hardening. For vessels operating in high-risk areas, the AIS's smooth operation should be examined regularly and the dedicated crew members should be well-versed with its use and functionalities.

There are many other solutions that can help crew to identify or prevent a piracy incident. For example, searchlights can be fitted in places offering all-round visibility while also deterring potential intruders. A single searchlight will not be able to give 360-degree coverage, therefore it is important to make sure that the existing lighting does not create areas of dead light (excessive shadow areas) that can conceal small vessels.

Images: Tatiana Popova/Shutterstock.com

In connection to the above, a vessel's lighting can be also used as follows:

- Weather deck lighting around the accommodation block and rear-facing lighting on the poop deck should be used.
- Search lights should be always readily available for immediate use.
- Once attackers have been identified or an attack commences, over-side lighting should be switched on to dazzle the attackers and help the ship's crew to see them.
- At night, only navigation lights should be exhibited.
- Navigation lights should not be switched off at night, as this a contravention of international regulations and the risk of collision is higher than that of being attacked.
- At anchor, deck lights should be left on – lit ships are less vulnerable to attack.
- The ability to turn off all internal accommodation lights to deter pirates from entering or disorientate those who may already have entered is recommended.

Once an attack is underway it may be difficult to assess whether the attackers have gained access to the ship. The use of CCTV coverage allows a degree of monitoring of the progress of an attack from a less exposed position. Some companies can monitor and record the CCTV from ashore. CCTV systems can be supplemented by audio devices, thus alerting the officer of the watch who can then hinder any attempts to either board the vessel or enter a restricted space.

Motion sensors can also be installed to warn crews of an attempted or actual intrusion/boarding and should only be used as an additional layer of hardening and not as a primary layer of defence. Motion sensors detect changes in the local environment, therefore, they can be active or passive.

Mounting anti-piracy mirrors can provide an efficient and cost-effective way of enhancing security onboard, eliminating blind spots and making navigation safer. Correctly positioned mirrors allow the watchkeeper to have a clear view from the bridge of the vessel's quarters areas, the whole of the stern sector (with overlap) and the propeller wake. The angle of the mirrors should be adjustable for best results. The housing and construction of mirrors should be robust enough to withstand all environmental conditions.

One other measure worth mentioning relates to restricting various vessel functions such as propulsion and lighting. Opting for a vessel blackout should then be considered, however a blackout should always be performed in a safe manner, ensuring at the same time that all other security measures/barriers will not be affected. Good arrangements and relevant training of the crew are essential to perform a blackout onboard.

What about cyber attacks?

Shipboard systems can protect crews against intruders. Given that many vessel control systems can be operated remotely, they may be susceptible to cyber attack. The use of electronic data exchange, including updates to navigational systems and software, exposes users to the possibility of unauthorised or malicious access. This creates a risk to the safety and security of shipboard systems. To protect commercial interests, as well as to ensure that safety and environmental protection are not compromised, it is important that seafarers comply with their company's cyber security procedures. Company procedures should take into account industry guidelines as well as any regulatory requirements addressing cyber security. It is advisable to invest in software security, ensure that the right processes are in place and followed and to ensure adequate cyber training is provided.

Training

Effective training will ensure vessel crew are adequately prepared for any possible security threat scenario and understand the prevailing threats in their regions of operation. The ship operator should ensure shore-based personnel have a basic understanding of the security threats that the fleet may face.

When developing or assessing a security training plan, the following points related to onboard threats should be considered:

- Briefing crew on the sequence of events and expected tactics employed in a typical piracy attack for the region of operation. This should include examples of recent incidents and lessons learned.
- Ensuring shore-based personnel complete training in crisis management, including family liaison, trauma support, kidnap and ransom procedures.
- Briefing crew on how the company would react to a piracy event, including the support mechanisms available for crew members' families.
- Briefing on how to behave in the event of being taken hostage by maritime criminals and the psychological effects this is likely to have on crew members.
- Implementing data security awareness for fleet and shore-based staff.

Risk assessment

Prior to transiting a high-risk area, a thorough risk assessment plan should be carried out to assess the likelihood and consequences of piracy attacks to the vessel. This should identify measures for prevention, mitigation and recovery, which will mean combining statutory regulations with supplementary measures to combat piracy. The process should take place according to the established company's risk assessment procedures, as described in detail in the company's safety management system and the SSP.

It should come as no surprise that vessels having a well-prepared and frequently drilled anti-piracy plan are less likely to be attacked or taken by pirates. Vessels that operate frequently or exclusively in high-risk waters are likely to experience a higher number of piracy incidents: however, if they are well prepared they may not be hijacked.

It is essential for crew members to be aware of the resources available in the vessel's "anti-piracy tool box". Simply, it all comes down to prevention and preparation. *MRI*

Elena Stefopoulou

Elena Stefopoulou, senior maritime advisor/analyst, Prevention at Sea

Tactical tips to minimise cyber attacks

Ken Munro, at Pen Test Partners LLP, outlines 10 tips for improving maritime security

The maritime industry is becoming increasingly more sophisticated in its use of new technology. Vessels and shore-based teams exchange data via satellite connectivity links to help optimise their operations with sensors measuring key performance indicators such as fuel consumption, route planning, and up-to-date weather forecasting.

Having internet access on board is also a key consideration for many crew members these days, particularly among younger crew, as they expect to be able to keep up to date with family and friends while at sea as well as being able to view digital channels and social media networks.

While this embracing of new technology by the industry is to be congratulated, this does leave it open to cyber attacks if basic cyber security protocols are not in place.

The industry has been hit with some major cyber security incidents in recent years. Probably one of the most high-profile cases was the ransomware NotPetya virus, which infected AP Moller-Maersk's IT systems in 2017. The company had to reinstall more than 4,000 servers, 45,000 PCs, and 2,500 applications with the overall financial loss estimated at US$300 million.

Ransomware was also the culprit which affected the US network of one of the world's largest shipping companies, COSCO (China Ocean Shipping Co). Staff had to resort to using public Yahoo email accounts to respond to customer enquiries via social media as the company's email and telephone network systems were affected.

> **"If respected blue-chip maritime organisations can fall victim to cyber attacks, then the whole industry needs to stop burying its head in the sand thinking it will never happen to them"**

Shipping broker Clarksons also admitted to a cyber breach where an unauthorised third party gained access to the company's computer systems in the UK and copied personal data for which the company received a ransom request for its safe return. Clarksons resolved the situation without paying the ransom but picked up all the costs for the implementation of identity protection for those affected by the security breach.

So, if respected blue-chip maritime organisations can fall victim to cyber attacks, then the whole industry needs to stop burying its head in the sand thinking it will never happen to them. Maersk's systems got caught up in a global ransomware attack but hackers will also target specific industries or companies which are easy to exploit due to lax cyber security protocols.

Pen Test Partners has highlighted multiple methods which can be used to interrupt and potentially cause chaos in the shipping industry by gaining access to a vessel's computer network via its satcoms terminal, exploiting key security flaws in the industry's top 20 ECDIS systems available on the market, hacking serial networks on ships and so on. Yet a lot of these vulnerabilities can be minimised if the industry adopted some very simple cyber security procedures.

One of the most common questions asked by ship operators is: "Where do we start with maritime security?"

In answer to that question, this article presents a list of the top 10 tips that every ship operator should employ right now to minimise the possibility of a cyber attack.

#1 Ensure your satcom isn't on the public internet

Most airtime providers offer a private IP address space, so hackers cannot reach your satcom system as easily over the internet.

It is easy to find out if your vessel terminals are public or not: put the IP address in a browser and see if you can route to the terminal web interface from the public internet. Or you could port scan it. Speak to your airtime provider and check.

#2 Check your satcom system has its passwords changed from the manufacturer's default

By far the most common problem: the satellite terminal installer has not changed the admin passwords from the default admin/admin or similar. Ensure the passwords are complex and only known by those who need to know.

#3 Update the software on the satcom system

Make sure it is at the latest version and ensure it is updated every time the manufacturer publishes an update. Updates usually include fixes for security flaws, so the more out of date the software is, the more vulnerable it is. Check the terminal vendors software updates pages regularly – security fixes are often hidden in the changelog and not easy to find. This takes time and effort, so to spare the legwork consider using a patch update alerting service.


kurhan/Shutterstock.com

#4 Check your bridge, engine room, crew, wifi and business networks on board are logically separated

If a device on your vessel is compromised, the presence of segregated networks will ensure critical systems are kept safe from the hacker.

Do crew members' personal laptops on the ship network have access to the navigation systems? Have you actually checked to make explicitly sure?

#5 Secure USB ports on all ships systems

It is very easy to accidentally get malware on USB keys. We have already seen cases of ECDIS and other systems compromised by ransomware introduced by mistake. How often do you see a phone charging from a USB port on a bridge console? Phones can be full of malware too.

To prevent accidental introduction of malware to vessel systems, lock down USB access. If critical systems can only be updated by USB, keep dedicated USB keys in a secure location that are used for nothing other this purpose. This is not ideal but is better than open USB access.

#6 Check all onboard wifi networks

Strong encryption, strong wifi passwords and good wifi router admin passwords are a must. Crew wifi for personal use must not connect to anything other than the internet and/or onboard systems (eg media streaming) for personal use.

Any ship systems that use wifi (eg tablets for comms and navigation) *must* have raised security levels, including stronger authentication.

#7 Do not rely on technology

Officers of the watch must be reminded not to rely too heavily on technology and get fixated on screens. GPS can be spoofed, ECDIS position can be manipulated and even synthetic radar can be hacked to misreport.

Whether it is navigation, collision avoidance or loading, the Mark 1 eyeball must be employed to ensure the situation outside the bridge reflects what the technology reports.

#8 Teach your crew about cyber security.

Resources such as "Be Cyber Aware At Sea" are great for raising awareness and helping your crew avoid inadvertently opening the vessel to compromise.

#9 Make your technology suppliers prove to you that they are secure

If you do not ask for security, you do not get it! Your technology and services suppliers will not spend any time on security if they do not think the market wants it.

A third-party audit of your supplier would be a good start, though in the short term you should ask for evidence of security accreditations such as ISO27001 or compliance with NIST (National Institute of Standards and Technology) cyber security frameworks.

#10 Get a simple vessel security audit carried out

Some of the worst vessel vulnerabilities are the easiest to find and fix. Bear in mind that maritime security issues are often systemic: they don't affect just one ship in your fleet, the same issue can affect them all.

While no company can be 100 per cent safe from cyber attacks, putting the above principles into action will certainly help to limit the chances of hackers gaining access to your computer network and should hopefully mean they will turn their attention to an easier target. ***MRI***


Ken Munro

Ken Munro, senior partner, Pen Test Partners LLP

Experience and seamanship to the fore when anchoring

David Nichol, at UK P&I, examines the potential impact of anchoring-related incidents, why they happen and what loss prevention measures may be implemented to prevent their occurrence.

The vast majority of ships are equipped with anchors and anchoring machinery that, apart from customary anchoring requirements, may also be used for manoeuvring or remain deployed if the ship is moored stern-to a berth or at an offshore terminal. The anchors may also be dropped to arrest the movement of a ship in emergency situations where control is lost due to poor manoeuvring or unexpected loss of propulsion, making them critical equipment.

Anchoring-related accidents can result in a wide range of potentially hazardous situations which may endanger the ship, life, property and the marine environment.

Anchor and cable loss

Most incidents reported to the UK P&I Club involve the loss of an anchor, often with all or a part of the cable. If the anchor is let go from the windlass brake in excessively deep water, the force of gravity will take over to the point where the brake is unable to arrest the momentum of the cable running out until eventually breaking free from the "bitter end" connection in the chain locker. This violent event can be very dangerous for the ship as well as for the crew located at the forward mooring station. The same situation can occur in any depth of water if the relative motion between the ship's bow and the ground is not carefully controlled by reasons of excessive manoeuvring speed, rate of turn, and the influence of wind and current. Even when the anchor is lowered (or raised) with the windlass motor engaged, the failure to minimise the relative movement between the bow and ground may result in catastrophic failure of the windlass machinery.

Loss of anchors can usually be attributed to incorrect anchoring practice or a deficiency in the anchoring equipment. A common reason for the loss of anchors and cables is failure of a linkage or shackle, with the "D" shackle joining the cable to the anchor, swivel link and Kenter type joining shackles being particularly vulnerable if not correctly assembled or maintained. As any chain is only as strong as the weakest link, the crew should take every opportunity to inspect the anchor cables between dry dockings to check for any deficiencies, including excessive wastage, wear and loose or missing link studs. Windlass motors, brakes and other fittings must be properly maintained in accordance with the manufacturer's instructions and should include periodic analysis of the windlass motor hydraulic fluid.

The replacement of lost anchors, cables and any associated repairs are required to be carried out under the supervision of the classification society. The local port authority will often demand anchors are recovered from the seabed, irrespective of the difficulty, which may incur considerable costs. There may also be sound economic reasoning for retrieving lost anchors for re-fitting on board.

Lost anchors and cables risk fouling other vessels anchors or causing bottom damage to hulls in shallow water. Claims for damage to sensitive underwater marine ecosystems such as coral reefs and electrical or telecommunication cables can easily run into millions of pounds. Damage to underwater pipelines may also risk the release of polluting contents.

Bringing a ship to anchor

To avoid the risks and costs already outlined, it is of the utmost importance that the anchoring operation is carefully planned by the bridge team in advance.

1. Planning

The master should have in mind the vessel may be required to anchor during the voyage, sometimes at short notice. Suitable potential anchorages should be identified and appraised during the passage planning process, which will include consulting the relevant navigational charts, pilot books, port guides and navigational warnings in advance. Charted designated anchorages are not necessarily suitable for all vessels in all circumstances. The seasonal and forecast weather conditions are particularly critical, as well as the exposure of the anchorage to weather.

Other planning considerations include the depth of water, nature of the bottom holding ground, prevailing currents and the proximity of navigational hazards in the anchorage. The anchoring position should be clear of any underwater cables, pipelines or other sensitive bottom features.

2. Water depth

A vessel should not be anchoring in water depths beyond the capabilities of the anchoring machinery. In accordance with typical minimum classification society requirements, the windlass is designed to lift the anchor and three shackle lengths of cable in the water (82.5 m). Although manufacturers will usually factor in an additional margin of safety, no unsupported assumptions should be made with respect to the lifting capability of anchor windlasses.

3. Holding power of the anchor

This will depend on the nature of the bottom and the length of cable paid out in the water. Clay, sand and shingle will provide better holding ground than soft mud or loose pebbles. Rocky bottoms or steeply sloping ground may be unsuitable for anchoring and increase the risk of the anchor becoming fouled on obstructions. The length of the paid out cable relative to the water depth – "scope" of the cable – should ideally be a factor of 6 to 10.

4. Anchoring manoeuvre

On approaching an anchorage, the master will need to assess where and how the vessel will anchor. It will require sufficient

jack_photo/Shutterstock.com

space to manoeuvre into the anchorage safely and adequate swing room, taking into account the weather, tide, current, traffic and the position of other vessels occupying the anchorage. The technique used to drop or lower the anchor, whether from the brake, under power or a combination of both, will depend on water depth and the nature of the bottom.

5. Master's criteria

Just because the master has been requested to anchor at a certain position by the port authority, pilot, or agent, does not mean that this advice should be followed blindly. If the master has good reason to believe that anchoring is not safe, the manoeuvre should be aborted and alternatives considered; whether that be a more suitable anchorage, drifting or steaming offshore in safe water.

6. Teamwork

Safely anchoring a ship requires good teamwork. The bridge and forward anchoring teams should be briefed by the master to ensure all concerned are aware of the intended anchoring plan and abort contingencies. The approach to the anchorage must be carefully executed and monitored; being alert to any unexpected traffic movements and avoiding crossing close ahead of other vessels at anchor. The officer in charge of the forward mooring team should ensure conditions at the bow, including the angle of lead and strain on cable, are promptly communicated to the bridge. On completion of anchoring, the chain stopper (or guillotine) must be properly engaged and locked.

Vigilance at anchor

With the ship safely brought up to anchor, there is sometimes a tendency for the crew to drop their guard and neglect good watch keeping practice during this period. The bridge team must be diligent in keeping a good lookout and closely monitoring weather conditions. The master should provide robust standing and night orders to officers of the watch on what is required of them should bad weather develop or be forecast as well as notifying the chief engineer of the required status of machinery readiness. The main engine should not be immobilised unless the safety of doing so has been subject to a thorough risk assessment.

If worsening wind and wave conditions are forecast, the master will need to consider additional measures to preserve the safety of the ship. When high wind and wave conditions are forecast, the master must consider departing from the anchorage in good time and steaming out to sea. Failure to do so will risk the vessel dragging anchor and difficulties in lifting the anchor cable, resulting in a dangerous loss of control. Anchors and windlasses are essentially fair weather equipment and it is imperative that ship's officers understand their environmental limitations.

If the officer of the watch notices the ship is dragging anchor, the master, duty engineer and other vessels at risk of collision must be informed immediately. As time is of the essence in such circumstances, the officer of the watch should be empowered to take prompt action to avoid imminent danger until the master arrives on the bridge.

Anchoring a ship is a routine yet critical operation, requiring the exercise of good seamanship developed through training and experience. Ultimately, it is the responsibility of the master to preserve the safety of the ship and crew; and to ensure commercial pressures should not influence decision making for safe anchoring. ***MRI***

David Nichol

David Nichol, senior loss prevention executive, UK P&I Club

Shipping and carbon: keeping pace with new rules

Paul Sheridan, partner, and **Valentina Keys**, at CMS, take a look at the UK approach to EU MRV Regulation and IMO DCS

As part of the European ship carbon reporting system governed by Regulation (EU) 2015/757 (the EU MRV Regulation) shipping companies had until 30 April 2019 to submit their ship emissions reports for relevant ships for the compliance year 1 January to 31 December 2018.

These reports were to contain data on CO_2 emissions; weight of cargo carried and/or the number of passengers carried (as applicable) and energy efficiency. They were to be provided to the European Commission and to the authorities of the flag state. From 30 June 2019 inspections of ships of ≥5,000 gt sailing into and between EU ports will include checks of whether a valid document of compliance (DoC) demonstrating conformity with the EU MRV (monitoring, reporting and verification) Regulation is kept on board. From 1 June 2020 ships will also need to have a statement of compliance on board to demonstrate compliance with the Global Fuel Data Collection System (IMO DCS).

Enforcement mechanism for the EU MRV Regulation in the UK

Member states are responsible for enforcement of the EU MRV Regulation. Sanctions for non-compliance with EU MRV differ across member states. The Merchant Shipping (Monitoring, Reporting and Verification of Carbon Dioxide Emissions) and Port State Control (Amendment) Regulations 2017 provide the enforcement mechanism for the EU MRV Regulation in the UK. The key point to note is that under the 2017 Regulations both the ship-owning company and the master of the non-compliant ship could be criminally liable for non-compliance.

For completeness, a "company" is defined in the 2017 Regulations (and this aligns with the EU MRV Regulation, article 3(d)), as the shipowner or any other organisation or person such as the manager or the bareboat charterer which has assumed responsibility for the operation of the ship from the shipowner.

Alex Kalokythas Photography/Shutterstock.com

"Under the 2017 Regulations both the ship-owning company and the master of the non-compliant ship could be criminally liable for non-compliance"

A DoC will be issued for each ship to be kept on board in readiness for inspections by local enforcement authorities and/or port state control which will commence from 30 June 2019. Failure to present a DoC to an inspection officer will expose the master of the ship and the ship-owning company to criminal and administrative sanctions including fines.

The potential fines should a relevant ship (1) enter or leave a port in the UK without a valid DoC; and/or (2) fail to keep on board a valid DoC or to present a valid DoC on inspection, are unlimited in England and Wales, and subject to the statutory maximum in Scotland and Northern Ireland. The current statutory maximum in Scotland is £10,000. The current statutory maximum in Northern Ireland is £5,000. In addition, the fact of a contravention will be published.

Otherwise, under the 2017 Regulations there are wide powers of enforcement including the power:

(a) to detain a relevant ship; and

(b) where a member state has informed the UK's Secretary of State that it has issued an expulsion order, refuse entry for the particular relevant ship to any port in the UK.

An expulsion order can only be issued by member states (including the UK) where a relevant ship has failed to comply with the monitoring and reporting requirements for two or more consecutive reporting periods and where other enforcement measures have failed to ensure compliance (article 20(3) of the EU MRV Regulation). Notably, the UK's Secretary of State has discretionary power to allow entry to a relevant ship that has been refused entry in limited circumstances. Provided the UK's Secretary of State is satisfied that adequate measures to ensure safe entry have been implemented by the company or master of the ship, the circumstances are:

(a) force majeure;
(b) overriding safety considerations;
(c) the need to reduce or minimise the risk of pollution; or
(d) the need to have deficiencies rectified.

Provisions for arbitration and compensation

The 2017 Regulations make provision for arbitration in the event that the master of the ship and/or the company alleges that a relevant ship was improperly detained. In the event that an arbitrator finds in favour of the master of the ship and/or the company following detention of a relevant ship, compensation will be payable in respect of any loss suffered in consequence of the detention of the relevant ship, should and as the arbitrator thinks fit.

"Special provision has been made by the UK in preparation for the UK's departure from the EU, intended to preserve the existing regulatory framework while laying down key changes to ensure effective operation of the MRV scheme in the UK"

Cooperation and information exchange

The EU MRV Regulation also requires member states to establish an effective exchange of information and effective cooperation between their national authorities responsible for ensuring compliance with monitoring and reporting obligations as well as those entrusted with penalty procedures. National penalty procedures against a specified ship by any member state will be required to be notified to the Commission, the European Maritime Safety Agency (EMSA), the other member states and the flag state concerned. The UK will no longer have such reporting obligations, when it leaves the European Union.

What about Brexit?

Special provision has been made by the UK government by virtue of the Merchant Shipping (Monitoring, Reporting and Verification of Carbon Dioxide Emissions) (Amendment) (EU Exit) Regulations 2018 in preparation for the UK's departure from the EU. The amended legislation is intended to preserve the existing regulatory framework while laying down key necessary changes to ensure effective operation of the MRV scheme in the UK.

The Explanatory Memorandum to the EU Exit Regulations explains that ships visiting ports in the UK will continue to be required to carry a DoC which will in future be issued under the UK regulatory framework. It further explains that UK regulators will continue to be able to enforce the MRV requirement to carry a DoC on board a ship against foreign vessels in UK waters, including EU vessels, and that DoCs issued under the EU regime will continue to be accepted in the UK. The Explanatory Memorandum also confirms that the new UK-governed MRV will no longer require ships to monitor and report on voyages which do not start or end at a port in the UK. Existing requirements on the UK to make certain reports to the European Commission will become redundant and all obligations to submit emissions reports to EU databases (eg Thetis MRV) will be replaced with a UK-based gov.uk website.

UK sanctions for non-compliance with IMO DCS

Similarly, one year from now, by the end of March 2020, as part of IMO DCS relevant fuel data of the first compliance period will need to be reported to the flag state. Assuming the reported data is in order, the flag state will issue a statement of compliance by no later than 1 June 2020 and will pass on the data to the IMO. It will be the responsibility of individual flag states to introduce appropriate enforcement measures to penalise non-compliance with the IMO DCS.

Most countries are in the process of implementing such measures. In the case of the UK, a senior policy advisor from the Department for Transport has explained that the domestic statutory instrument to implement the IMO DCS is still being drafted and is to be laid before Parliament in the next couple of months. He also confirmed that the main focus of the Maritime and Coastguard Agency (MCA)'s enforcement efforts in relation to the IMO DCS regime will be checking if non-UK ships have a valid SoC to confirm that they have collected the required fuel consumption data for the year concerned when they call at a UK port.

The first of these statements will be issued in 2020. UK-flagged ships will have to satisfy MCA surveyors or organisations authorised to act on behalf of the MCA, that they have the appropriate documentation and procedures in place to comply with the IMO DCS, when they are next surveyed. Fines for non-compliance are likely to be similar to those levied under the 2017 Regulations.

Comment

Of course, it will take a little while before any patterns may emerge in terms of: (1) compliance and enforcement (in the UK and elsewhere); and (2) what use (maybe in terms of subsequent tightening legislation, or introduction of economic or other incentives or disincentives) regulators and legislators will make of the information that is gathered. ***MRI***

Paul Sheridan

Valentina Keys

Paul Sheridan, partner, and Valentina Keys, senior associate, CMS

Water, fuel, gases, boats and ships … and the unexpected vapour problem

Chris Roberts, of Versaperm, reports on the way new technology is helping with some age-old problems

We are all familiar with the effect liquids have on the things we encounter in our everyday lives: cornflakes that go soggy if you do not eat them quickly enough, engines that won't start properly and shoes and clothes that either aren't waterproof, or won't get rid of perspiration even on a cool and cloudy day.

The issue actually goes much deeper and is of very specific concern to the marine world where water, fuel and various other liquids are not only plentiful but can cause great harm if they get into the wrong places. The difficulty is that neither water nor hydrocarbon vapours behave as well as they do when they are liquids. As vapours they can permeate through any and every barrier, seal or enclosure; they seep through the very materials that things are made from – and at a rate that costs the UK alone several billion pounds a year.

> **"The onboard presence of vapours like water or hydrocarbon vapour, hydrogen, solvents and CO_2 can cause chaos in electronic equipment and lead to serious damage and the unexpected failure of safety-critical or navigational equipment"**

A good analogy to explain this is breathable fabrics, such as Goretex, which prevent liquid water from passing through, but allow air and water vapour to move through freely and escape. Similarly, there are many materials we regard as excellent barriers to water, but which allow water vapour to penetrate with very little barrier effect. Silicon is a good example of this – like most plastic polymers it keeps liquids out – but as for vapours such as water or oxygen it is so poor that sometimes it might just as well not be there at all. It allows around 100,000 times more water vapour through than, for example, either polyethylene or nylon. Many other common materials, including EVOH, PVOH and cellulose can be equally poor.

The onboard presence of vapours like water or hydrocarbon vapour, hydrogen, solvents and CO_2 can cause chaos in electronic equipment and lead to serious damage and the unexpected failure of safety-critical or navigational equipment. It can even happen without the crew even knowing that there is a problem until it is too late and a system fails. There are many other problems, such as equipment that jams or paper that you cannot write on properly. To be fair this is true in many areas – but it is worse in the marine world as there is a far greater supply of water and fuel to cause problems.

Sometimes, the easy flow of vapour can be a good thing – for example in wound dressings, in breathable shipboard clothing, the wrappings around some foods and the preservatives used on some woods – but usually it just causes problems.

And the problem continues when it comes to fuel. Sensibly there are strict regulations regarding the allowable vapour permeability characteristics of fuel tanks from just about every country in the world. However, serious glitches have been caused by piping, tubing and components that allow hydrocarbons to leach through.

The problems and potentials, like the vapours themselves, are ubiquitous and it is sensible to understand a little more about how permeability is measured, how different materials are more suited to individual jobs and how the new breed of "designer" materials such as multi-layer laminates or coatings, can help bring new solutions to these age-old problems.

Testing

Generally speaking, today's testing processes involve a standard (or range) of temperatures/pressures and a barrier made from the material under test, with a high humidity or high fuel vapour concentration on one side. The rate that the vapour flows through the barrier is then measured on the other side. Nowadays it will be swept up by an inert gas and carried to a sensor.

There is a huge range of these sensors available depending on the required sensitivity and gases, and there are even some sensors – such as mass spectrometers, that can measure several gases at a single time.

However, there is a snag, as many of the national and international standards have not yet caught up with modern instrumental techniques and are still based on an old "gravimetric" technique. This requires measuring the weight gain of a water or hydrocarbon-absorbing material on the "dry" side of the barrier. The tiny weight gain relates to the amount of vapour that passed through. Modern techniques are accurate, faster and more practical – especially as the time taken to produce gravimetric results is typically weeks or even months!

Modern instruments are practical, flexible and give very accurate results for most materials and gases. As well as mass spectrometers techniques these can, for example, use Faraday's law to measure a current that is passed through gas on the dry side of the meter. This is directly and absolutely related to the number of water vapour molecules that have passed through the material – and a precise measurement can be made, sometimes in as little as half an hour.

One caveat of warning is that there are many different ways of expressing the units used to measure vapour permeability and different industries and countries tend to use different units. This causes great confusion as not only are measurements from the US usually expressed in different units from those used in

Vapour-barrier materials relative water vapour permeability (based on polyamide at 100 per cent)	
Material	**Relative water vapour permeability**
Polyamide (PA or nylon)	100
Acrylonitrile copolymer (Barex)	20
Polyvinyl choride (PVC)	16
Low vapour-barrier materials	
Polyethylene terephthalate (PET)	5.2
Low-density polyethylene (LDPE)	4.8
Good vapour-barrier materials	
Polypropylene (PP)	1.6
High-density polyethylene (HDPE)	1.2
Polyvinylidene chloride (PVDC or saran)	0.2
Polychlorotrifuoroethylene (PCTFE or Aclar)	0.16
COC	0.24 to 0.29
CTFE	0.02
Cold Form Foil	0

Europe, but also electronics enclosures can even be measured in different units to fuel tanks. All of the units relate and can be converted, but the possibility of confusion reigns supreme.

So, we can now move on to look at various commonly used materials and situations to see how they respond to water vapour.

Films

Most polymers offer very good resistance to both fuel and liquid water though unexpectedly there is little correlation between the vapour permeability of a material for water and hydrocarbon vapours. A material that is good in one case, might have little effect on the other. Some of the best polymeric barriers to water vapour include PVDC (polyvinylidene chloride) and PCTFE (polychlorotrifluoroethylene). The least permeable films are laminates which include a component of aluminium, either as a discrete layer or as a result of a metalisation process.

Coatings

Coatings are often required to protect an item from water or hydrocarbons both as liquids and as a vapours, for example to protect wood from swelling and splitting or to protect metals from corrosion. The testing of a coating for vapour permeability is relatively simple and can typically be completed within an hour. It may also come as a surprise that it is possible to use coatings that offer, for example, poor liquid water resistance, but good water vapour barrier properties.

Tubing

While metal tubing is largely impervious to vapours, most types of plastic tubing permit some vapour to pass through. This is significant for certain applications and can be serious in safety-critical areas. The testing of plastic tubing often provides unpredictable results due to differing manufacturing techniques.

Sealants and mastics

Sealants and mastics are both widely used and have a huge range of chemical compositions. Although acting as a barrier to liquids is one of their main functions, they vary enormously in their resistance to vapour. This can be easily overlooked as the automatic, but fatally flawed first assumption, is that if they stop liquid, they stop vapour as well.

Gaskets, O-rings and foam seals

Again, there is a wide range of these materials, each appropriate to the designed application. In this case there is usually a requirement to place a material under a specified level of compression to achieve the appropriate barrier. This makes testing more specialised. Different compression levels offer different resistance to water vapour, either too much or too little can reduce effectiveness, and the only way to check this is to measure each individual product.

Containers

There are several potential paths for vapour to take when entering or leaving a container and there is the risk of leakage between the seals and the container or closure. This will often depend on the closure being correctly torqued. Instrumental techniques are commonly used for measuring the vapour permeability of containers ranging in size from eye-droppers to 25-litre drums and beyond.

"Although acting as a barrier to liquids is one of the main functions of sealants and mastics, they vary enormously in their resistance to vapour. This can be easily overlooked if the assumption is that if they stop liquid they stop vapour as well"

Designer coatings

With the latest measuring technology, we now have the ability to custom-design coatings to give materials a specific range of properties depending on the specific needs of the applications. Designer coatings are already used to boost the shelf life and effectiveness of food, drinks and drugs and are now moving into specialist fields – such as preventing electronics from failing in the marine environment or coatings that dramatically reduce rusting and fouling. It is also important as even slight changes to manufacturing process can make a big difference – for example even simple thermoforming can change the vapour permeability of a material by a factor of four from its original value.

It is startling to realise just how many marine applications and systems are affected by water, hydrocarbon or other vapours – this is especially important because systems failure can occur before a crew even knows there is a problem. But once you know where to look, the rest is just plain sailing. ***MRI***

Chris Roberts

Chris Roberts, director, Versaperm

Fire in the hold

It is over a year since the *Maersk Honam* casualty but fires on containerships continue to occur. Now container shipping is making efforts to reduce the risks, writes *Lloyd's List*'s **James Baker**

Just over a year on from the fatal fire on *Maersk Honam*, the container shipping sector has little to boast about in terms of improvements to its safety record. This year alone has seen further cargo fires on boxships, including those on Hapag-Lloyd's *Yantian Express*, *APL Vancouver*, and Grimaldi's con-ro *Grande America*. Fortunately, none of these included fatalities, but in the case of *Grande America*, the vessel was lost when she foundered in the Bay of Biscay.

According to cargo insurer the TT Club, a containership fire at sea happens once every two months on average. While it might be tempting to blame container shipping as a sector for this appalling record of safety, in most cases the real blame lies with customers rather than the lines themselves.

Although the specific causes of all the casualties, including and since *Maersk Honam*, remain unknown, misdeclared cargoes of dangerous goods are suspected in each of them. In one infamous casualty where the cause has been determined, the blame has been squarely laid at the feet of the cargo owner and forwarder.

The court judgment in the *MSC Flaminia* damages claim found that the owner, operator and shipmanager of the vessel were all exempt from liability, which lay instead with the cargo owner, Deltech, and to its non-vessel operating carrier, Stolt Tank Containers.

That case centred around the poor handling of a known dangerous cargo, divinylbenzene, which is at risk of auto-polymerisation when heated. It was allowed to sit on dock for 10 days in hot weather conditions before being loaded, allowing it to deteriorate.

The court found that there had been poor communications between the forwarder and the carrier, Mediterranean Shipping Co. Despite knowing of the cargo's propensity, Stolt had not warned MSC of the risk from its storage.

"Carriers cannot be expected to check every container loaded onto a vessel. Moreover, with vessel-sharing agreements, the cargoes on a carrier's ship often will not even have been booked through that carrier. Tracking down a misdeclared cargo is fraught with difficulty"

Although in this case the content of the container had been declared, in many cases, carriers are unaware of what is in containers on board their vessels.

TT Club says there are potentially 1.3 million unstable dangerous goods containers shipped every year. Citing cargo handling operatives body the International Cargo Handling Coordination Association estimates, TT Club says about 10 per cent of the 60 million loaded containers moved each year are declared as containing dangerous goods. Of these, information from published government inspections suggests that 20 per cent are poorly packed or incorrectly identified, amounting to 1.3 million risky boxes. Moreover, 150,000 boxes a year may contain misdeclared cargoes.

Figures collated by German container line Hapag-Lloyd indicate that across the industry, 0.06 per cent of all containers

Maersk Honam


MSC Flaminia

carry undeclared dangerous goods. While that may be a small percentage, in a port such as Singapore, handling 20m teu a year, it represents 12,000 containers that could contain undeclared dangerous goods. The 2015 fire and explosion at Tianjin that killed 44 people demonstrates the possible impact of such misdeclarations.

Carriers cannot be expected to check every container loaded onto a vessel. Moreover, with vessel-sharing agreements, the cargoes on a carrier's ship often will not even have been booked through that carrier. Tracking down a misdeclared cargo is fraught with difficulty.

Hapag-Lloyd developed its own software in-house in an effort to solve one of the potential pitfalls, the use of synonyms for dangerous goods. Calcium hypochlorite, an unstable oxidising agent that can readily ignite if not stored correctly, has about 20 synonyms, including innocuous names such as bleaching powder.

Grande America

Cargo Patrol, which Hapag-Lloyd developed then gave to IBM for wider industry adoption, scans the booking environment in real time to detect any undeclared dangerous goods or suspicious cargo.

But the sector is now understood to be looking at a wider solution to the problem of misdeclared cargoes. A group of leading container lines is thought to be preparing a new industry-wide initiative and considering a range of options, including legal action against shippers or forwarders that misdeclare dangerous cargo, and a standardised approach to handling hazardous freight.

But for TT Club risk management director Peregrine Storrs Fox, responsibility needs to be taken by the entire supply chain. The club has launched its Cargo Integrity campaign, which aims to focus the container supply chain sector on safety issues related to the incorrect processing of dangerous goods.

"We are endeavouring to focus all direct and indirect stakeholders on recognising and doing the right thing," he said. "There is very much still to be done in achieving true Cargo Integrity. Above all, there is a need for all involved in the supply chain to have a realistic perception of risk and a responsible attitude towards liability."

Multi-pronged approach urged to solve hazardous cargoes problem

Suggestions range from revising the relevant codes to updating the International Convention for the Safety of Life at Sea to keep up with the demands of larger container vessels. However, the pressure on costs was also raised as a contributory factor to hazardous cargoes being mislabelled, writes Lloyd's List's Vincent Wee

The problem of hazardous cargoes is a multi-faceted one and there is not really a single-pronged approach that can be taken to the problem, a panel of speakers at an Asia Maritime briefing in Hong Kong suggested.

Technical experts such as Hawkins regional director John Allum and ABS director, Market Sector Containerships Jan Otto de Kat focused more on the practical side of things to reduce the risk of incidents.

For example, simplifying the relevant IMDG and IMSBC codes might be a start, suggested Dr Allum. He pointed out how even he and his fellow experts needed many hours to understand these codes and what they entail and related how it might be unnecessarily difficult for shippers to comply. "If we could go back and say here's a simple code for shippers and this is what you need to do, it would make everything much more practical," he said.

Mr de Kat suggested looking at the issue from a risk-based perspective and with that it would emerge that greater risk would naturally arise from the larger container ships. Following on from this, he noted that the current Safety of Life at Sea Convention requirements may not have kept up with the rapid developments in terms of ship sizes in container shipping in particular.

From the commercial side, American P&I Club Shanghai managing director Dimitris Seirinakis pointed out that many of the problems now arising with hazardous goods are being caused by consumer demand and the vast amount of goods being transported around the world.

This has led to the building of bigger ships with an accompanying rise in risk. Mr Seirinakis suggested that in the same way that the dry bulk sector has introduced dedicated ore carriers that are better able to deal with the problem of liquefaction, perhaps the container liner industry should consider building smaller container ships that are dedicated to carrying dangerous goods.

He said these vessels could have more specialised firefighting equipment and specifically-trained crew for example.

The rub is of course, that this is set against the backdrop of falling freight rates as the industry gets commoditised. "If we were to look at beginning to solve this problem I would say that we need to be paying more for our transport in order to be able to sustain a safe shipping environment," commented Stephenson Harwood partner Andrew Ridgen Green.

Mr de Kat also harked back to the very low rate environment as being a big cause of the problem. The question is whether there can be a change in thinking for society to accept a somewhat higher cost to get safer shipping, he concluded.

Lloyd's List
Maritime Intelligence | Informa

This article first appeared in our sister publication *Lloyd's List*. For more, visit www.lloydslist.com