Marine Hull & Machinery and War Risks Market Update

FEBRUARY 2018

Gallagher

Insurance | Risk Management | Consulting

About Gallagher

Founded by Arthur Gallagher in Chicago in 1927, Arthur J. Gallagher & Co. has grown to become one of the largest insurance brokerage and risk management companies in the world. With significant reach internationally, the group employs over 26,000 people and its global network provides services in more than 150 countries.

Globally we use the brand name Gallagher

Contents

01. INTRODUCTION

Welcome to the February 2018 edition of the Gallagher Hull & Machinery and War Risks market report.

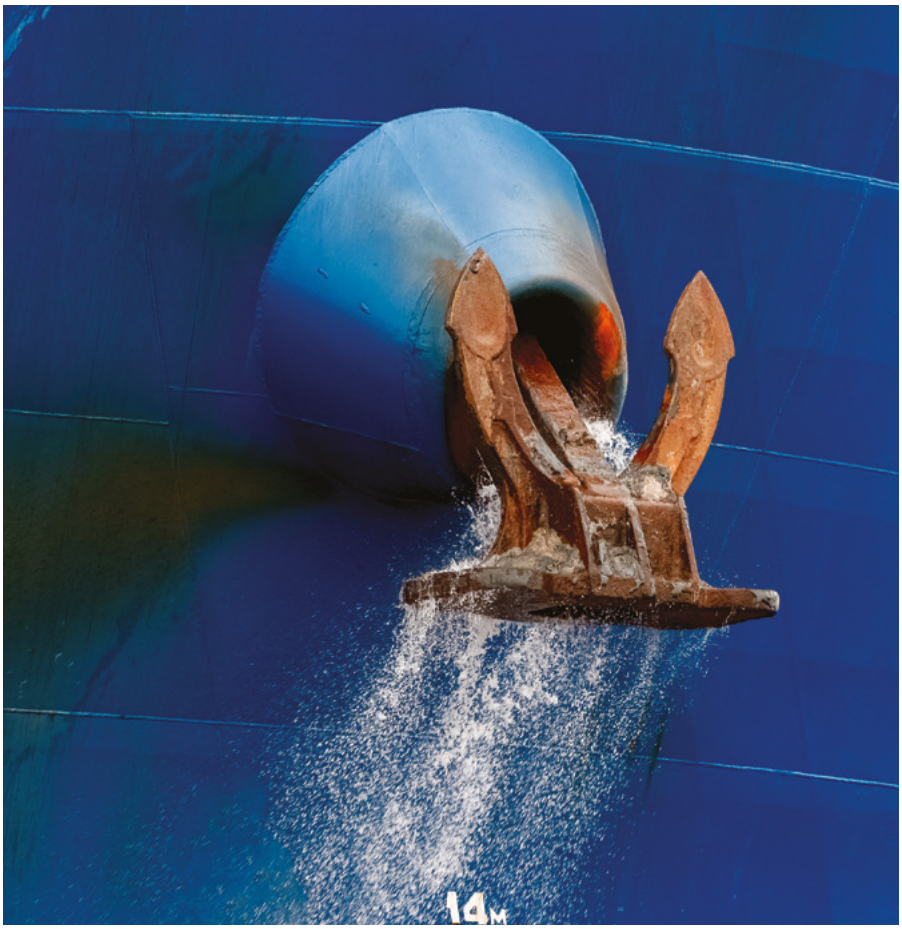
The latter part of 2017 was characterised by a tougher stance on renewals from a number of Underwriters. The continued negative results on the overall Hull & Machinery portfolio have been the main contributory factor, however, the major natural catastrophes of 2017 have undoubtedly affected the international insurance market as a whole and have provided a catalyst for change in individual poor performing areas. 2017 is widely reported as the most expensive year on record for US natural catapstrophes which included Hurricanes Harvey, Irma, and Maria, as well as the extensive wild fires in California, and the earthquakes in Mexico in 2017. Whilst commercial marine H&M losses from these catastrophes are not significant, marine Underwriters have suffered huge losses on their yacht portfolios and also on cargo, especially goods in storage in the Caribbean and East Cost United States.

In spite of the above, the Hull & Machinery market is still characterised by plentiful capacity for international business. There has been no meaningful retraction of capacity as yet and although the market is undoubtedly stabilising, there are no short term signs of a significant hardening.

Cyber Risk has been a hot topic in 2017 and addressing the exposures faced by the shipping community will continue to be a top priority this year. We are working closely with our clients to identify and manage exposures whilst at the same time addressing these exposures with Underwriters in order to find insurance solutions where possible. In this report going forward, we will be presenting recent news articles related to marine cyber related incidents alongside the usual casualty and war/ piracy reports.

02. MARKET MOVES

Jonathan Humm will shortly leave Hiscox Syndicate to take on a new role as the Marine Hull Underwriter at Aegis Syndicate.



03. CASUALTY REPORTS

The "Sanchi" burning following the collision with CF Crystal

Sanchi / CF Crystal Collision

The Iranian tanker Sanchi sank on 14th January 2018, after burning for over a week following a collision in the East China Sea according to Worldmaritimenews.com. The tanker collided with the Hong Kong flagged bulk carrier CF Crystal on 6th January 2018 and drifted according to China's Ministry of Transport about 65 nautical miles, into Japan's exclusive economic zone, some 300km northwest of Sokkozaki on the island of Amami Oshima. She finally sank 310km from Naha Japan. The tanker was carrying 136,000 tons, the equivalent of 1 million barrels, of ultra-light crude oil, and suffered an explosion around 12 o'clock on 14th January 2018 which led to the vessel sinking. The estimated value of the cargo was US$60 million.

World Maritime News reported that before the tanker sank, Mohammad Rastad, spokesman of the Iranian rescue team dispatched to Shanghai, told Iran's state news agency that, "despite our efforts, it has not been possible to extinguish the fire and recover the bodies due to repeated explosions and gas leaks."

According to insurance marine news the ship's crew of 30 Iranians and two Bangladeshis were probably killed in the first explosion. Three bodies have been later recovered and identified.

The aftermath of the explosion

According to Reuters almost two weeks after the vessel sinking, authorities were puzzled about the size of the oil spill, as it changed by the day amid several strong ocean currents including the powerful Kuroshio. Concerns were growing about the potential impact to key fishing grounds and sensitive marine ecosystems off Japan and South Korea, which lie in the projected path of the oil, according to Britain's National Oceanography Centre.

On 18th January 2018, almost two weeks after the collision, there were four separate oil slicks of the condensate from "Sanchi" which together cover over 100 square kilometers, or just under 40 square miles, the same size as Paris, according to a statement released by the Chinese State Oceanic Administration reported by Ecowatch.com

National Geographic reports that the type of oil that was spilled into the East China Sea is unlike other major oil spills and there are a lot of unknowns including the size of the spill, its chemical makeup, where the chemicals from the oils will spread, making it difficult to predict the impact on the environment.

Unlike crude oil, which can create chronic environmental problems by sinking to the deep ocean and lingering there for years, hydrocarbon condensate is much lighter, evaporating or dissolving into water. That means short-term toxicity might be a bigger concern with this spill. Ralph Portier, a marine microbiologist and toxicologist at Louisiana State University in Baton Rouge says that "most oil spills have a chronic toxicological effect due to heavy residuals remaining and sinking over time," (Nature.com) "This may be one of the first spills where short-term toxicity is of most concern." A significant, but unknown, portion of the Sanchi's condensate probably fueled the fires that followed the collision. In the waters immediately surrounding the tanker, Portier says, the conflagration and gaseous fumes would have killed off or injured phytoplankton, along with birds, marine mammals and fish that were caught in the vicinity when the tanker ignited.

Japan Times reported that the Cabinet Office announced on 1st February 2018 a branch was established to monitor information about the oil spilled. The central government's action comes a day after the Japan Coast Guard and Kagoshima Prefecture confirmed that black oily substances were found drifting ashore on the small island of Takarajima, which lies between Amami Oshima and Yakushima, a world heritage site famous for its ancient cedar trees. "Cleanup operations in and around the Amami Oshima area have been taking place. Right now, there is no official confirmation yet that the oily substances are from the tanker, but we'll continue to monitor the situation," Yuta Nishikawa, a coast guard spokesman in Kagoshima, told The Japan Times on Friday.

Photo: 10th Regional Coast Guard Headquarters/Handout via REUTERS

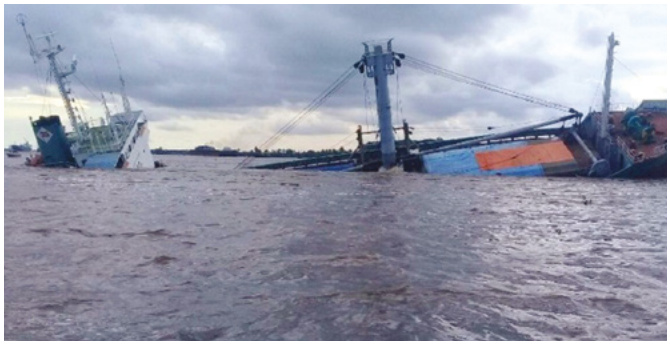
Qi Cheng Xian Feng

On 4th December 2017, the 54 meter long coastal tanker Qi Cheng Xian Feng sank after having run aground at low tide and sustaining multiple hull breaches, according to Shipwrecklog.com. With the rising tide, the Qi Cheng Xian Feng later sank by the stern. All crew managed to escape the sinking boat. There were no reports of injuries or pollution.

Genessa Fire

Rooselaw reported on their casualty newsletter No. 252 that on 17th January 2018 a major fire erupted, following an explosion in the portside of the crude oil tanker Genessa off the coast of Kandla in Gujarat, India. The crew of 26 and the Master were evacuated from the vessel but two of the crew were seriously injured suffering from burn injuries, one of whom later died.

Coastguard vessels and 10 tugs that were dispatched in the area, but were moved back from the vessel in view of safety concerns that water might catch fire and compromise tugs' safety. Some of the tugs were able to spray their water monitors on to the tanker, which adopted a slight port list. The fire was extinguished after 28 hours of firefighting and no loss of cargo was reported. According to insurancemarinenews.com the cause of the fire appears to be a leak of furnace oil in the engine room.



Keneukai Sank

The 1984 built General cargo vessel "Keneukai" sank in Port of Trisakti on 8th December 2017. According to worldmaritimenews.com the ship dragged anchor, but before the crew could start the engines she hit a submerger wreck. The ship finally sank following water ingress from a hole in the hull. She was carrying approximately 2,500 tons of cement at the time of the incident.

04. WAR AND PIRACY NEWS

Six crew members kidnapped

21st October 2017

The fully cellular containership Demeter (Built 2006, 41,647 dwt) was attacked by pirates on 21st October 2017 in the Gulf of Guinea south of Port Harcourt, Nigeria whilst en route from Malabo Equatorial Guinea to Monrovia, Liberia. Six of her crew were kidnapped, including the Master and Chief Engineer. The kidnapped crew were released three weeks later according to Rooselaw (Casualty newsletter no.242). At that time it was not clear whether a ransom was paid.

Pirates target Crude Oil Tanker off Nigeria

3rd November 2017

A Crude oil tanker managed to escape pirate hands while sailing some 21 nautical miles South-Southwest of Bonny Island, Nigeria on 1st November 2017 according to worldmaritimenews.com. The tanker was approached by armed pirates in two speed boats at high speed, according to the IMB Piracy Reporting Centre. "The officer of the watch immediately raised the emergency alarm and the master notified the terminal who relayed the information to a Nigerian naval ship," IMB said. The master ordered the crew to secure all access to the vessel and retreat into the citadel. The pirates' attempts of boarding the tanker by using a ladder as they closed in on the vessel were thwarted by the bridge team who resorted to evasive maneuvers. Shortly after, a Nigerian naval vessel arrived at the scene causing the pirate group to abandon their hijacking attempt. "On seeing the approaching naval ship, the pirates aborted the attempted boarding and moved away. The tanker continued its passage," IMB further added. All crew members are reported to be safe.

WORLD MARITIME NEWS STAFF

Attack on bulk Carrier "Venus Bay"

15th November 2017

The 30,003 ton 2012 built bulk carrier Venus Bay was boarded by pirates in the Bight of Bonny who damaged the vessel and kidnapped ten of the crew. The Nigerian Navy ships intercepted their boat and freed the crew, taking the pirates into custody. The vessel was escorted to Port Harcourt.

Tanker released after 6 day hijack

10th January 2017

The tanker 'MT Barrett' has been released from pirates, after captivity of six days, with all 22 crew reported as safe. The crew were safely back in Lagos, Nigeria according to an official statement by Union Maritime, the owner company. The missing tanker had been subject of a piracy attack in Gulf of Guinea, since 10th January 2018, after all communications were lost.

Union Maritime's emergency response plan was immediately activated and regional maritime authorities and other vessels in the area were alerted. "The exact nature of the incident only became clear late on 12th January 2018 when those holding the vessel made contact with the company. A resolution process began, which ultimately led to the release of the vessel and all crew on board on 16th January 2018," the company added.

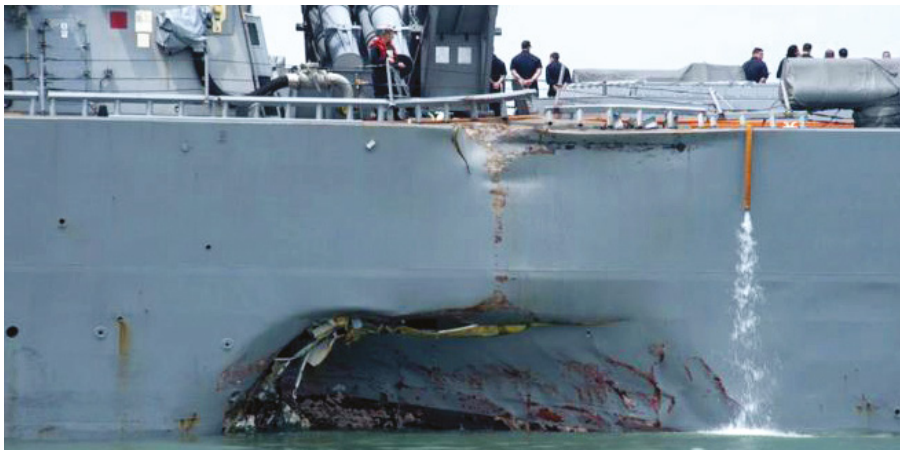
Second vessel disappeared in Benin within a month

1st February 2018

The 45,000 ton oil tanker "Marine Express" was reported missing on in the Gulf of Guinea, off Benin according to BBC. The incident came shortly after the 'Barrett' was captured and subsequently released by pirates in the same area. At the time of her disappearance the Marine Express was carrying 13,500 tonnes (15,120 tons) of gasoline. According to the vessel managers, as reported on Sky News the last contact was at 03:30am, 1st February 2018. As at 5th February 2018 the vessel was still missing.

Missing oil tanker "Marine Express

05. CYBER RELATED NEWS



The USS John S McCain collided with a tanker

Cyber-attack alert weeks before USS John S McCain warship crashed

Richard Kerbaj, Security Correspondent
27th August 2017, 12:01am,
The Sunday Times

Ship owners were warned about the threat of cyber-attacks only weeks before America began investigating the "possibility" that hackers caused the collision between one of its warships and an oil tanker, The Sunday Times can reveal. The International Maritime Organisation (IMO), a London-based UN-affiliated body that regulates shipping, last month published guidelines urging ship owners to safeguard vessels against the "current and emerging threats" of cyber-hacking.

This weekend Lord West, a former admiral in the Royal Navy, also raised concerns about cyber-attacks, saying he was worried by merchant vessels' vulnerability. The revelation follows the collision between the American destroyer USS John S McCain and a Liberian oil tanker, Alnic MC, in the South China Sea last week, leaving 10 US sailors dead or missing.

The route of the tanker, taken from tracking signals and posted online by the VesselFinder website, shows it making a sudden turn to port just before the collision. Military intelligence officials fear the tanker may have been sent off course by a remote attack on its navigation systems. It was the fourth time a US warship has been involved in an accident in Asian waters this year, raising questions about possible interference by state-sponsored hackers, sources say.

The US defence department warned in last year's annual report about China's use of "electronic warfare" as a way to "reduce or eliminate US technological advantages". It said Beijing's capabilities included "jamming equipment against multiple communication and radar systems and GPS satellite systems".

Zhang Zhaozhong, a rear admiral in China's People's Liberation Army, celebrated the collision of the USS McCain, accusing the ship of "making a lot of trouble in the South China Sea . . . what goes around comes around". The IMO's new guidelines describe "an increasing need for cyber-risk management in the shipping industry".

It is the second time it has warned about cyber-attacks, after a 2014 paper revealed that "state-sponsored hackers, terrorists and other malicious actors have turned towards exploiting weaknesses in cyber-security". Peter Roberts, a cyber-expert who runs the military sciences unit at the Royal United Services Institute, said: "The offensive use of cyber has tended to follow the doctrine of electronic warfare of old. Competitor states — China, Russia, Iran, North Korea amongst others — continued to develop and invest in their electronic warfare capabilities . . . and now [that] means they have a competitive advantage."

Computer hackers targeted BW Group

Incident at Singapore shipowner came less than a month after ransomware attack on Maersk.
16th October 2017, 02:15am

BW Group has been targeted by computer hackers, the Singapore-based shipowner has confirmed to TradeWinds. "We had an unauthorized access and actions have been taken to rectify the matter," a BW Group spokesperson confirmed to TradeWinds. "Internal and external communications to customers and stakeholders were not impacted and it was business as usual with some inconveniences as we worked around planned system downtimes as our IT department, with assistance of external consultants, reinforced our cybersecurity infrastructure." The incident is said to have taken place in July, just one month after the ransomware attack on Danish shipping giant AP Moller Maersk. However, the BW spokesperson said the cyber-attack on the company's computer systems was not ransomware. The spokesperson did not divulge information on any financial or data loss due to the unauthorized external access, or whether the culprits had been identified or traced. "The active directory and GPO systems were affected and the problem was serious enough for Internet and Intranet systems to be closed down temporarily," a sources familiar with the matter told Platts, who first broke the story. Sources quoted by the wire agency said that an audit of BW's computer systems was conducted by KPMG, which undertook forensics pertaining to the entire incident. A report earlier this year by Norton Rose Fulbright said that more cyber-attacks are anticipated as shipping sets its sights on increased digitalization. Meanwhile, an anonymous cyber-crime reporting site for the maritime industry is set to go live this month in a tie-up between Airbus and the CSO Alliance. The European aircraft manufacturer will run the site, which has been developed by the alliance for company shipping security officers. The portal will provide alliance members with cyber-security information, news of incidents and advice on how to handle them, plus live data.

Israel's Naval Dome demonstrates hack attack on ship's controls

3rd January 2018,
Insurance Marine News

Israel-based cyber security company Naval Dome said that it had demonstrated a hack – with the permission of the owner and the system manufacturers– into live, operational systems used to control ship's navigation, radar, engines, pumps and machinery, reported Schednet.

The team hacked into computer systems which owners are legally obliged to use to control their ships. Naval Dome software engineers say they were able to shift the vessel's reported position and mislead the radar display. Another "attack" resulted in machinery being disabled, signals to fuel and ballast pumps being over-ridden, and steering gear controls being manipulated.

"We succeeded in penetrating the system simply by sending an email to the captain's computer," said Naval Dome chief technical officer Asaf Shefi.

"We designed the attack to alter the vessel's position at a critical point during an intended voyage - during night-time passage through a narrow canal," said Mr Shefi, former head of the Israeli Naval C4I and cyber defence unit. "During the attack, the system's display looked normal, but it deceived the officer of the watch. The actual situation was completely different to the one on screen. If the vessel had been operational, it would have almost certainly run aground," he said.

The Naval Dome hack altered water depth in line along with the false position data displayed on screen. "The vessel's crucial parameters - position, heading, depth and speed - were manipulated in a way that the navigation picture made sense and did not arouse suspicion. This type of attack can easily penetrate the antivirus and firewalls typically used in the maritime sector," Mr Shefi said. He noted that the captain's computer was regularly connected to the internet through a satellite link, which was used for chart updates and for general logistic updates. The attacking computer file was transferred to the Electronic Chart Display and Information System (ECDIS) in the first chart update. It then identified the disk-on-key use for update and installed itself. Thus, once the officer had updated the ECDIS, the attack file immediately installed itself on to the system.

In a second attack, the test ship's radar was hit. While the radar is widely considered an impregnable, standalone system, Naval Dome's team used the local Ethernet Switch Interface - which connects the radar to the ECDIS, Bridge Alert System and Voyage Data Recorder - to hack the system.

"The impact of this controlled attack was quite frightening. We succeeded in eliminating radar targets, simply deleting them from the screen. At the same time, the system display showed that the radar was working perfectly, including detection thresholds, which were presented on the radar as perfectly normal", said Mr Shefi.

A third controlled attack was performed on the Machinery Control System (MCS). Naval Dome penetrated the system via an infected USB stick placed in an inlet/socket. "Once we connected to the vessel's MCS, the virus file ran itself and started to change the functionality of auxiliary systems. The first target was the ballast system and the effects were startling. The display was presented as perfectly normal, while the valves and pumps were disrupted and stopped working. We could have misled all the auxiliary systems controlled by the MCS, including air-conditioning, generators, fuel systems and more", said Naval Dome CEO Itai Sela. He also warned that manufacturers themselves could be targeted when they took control of onboard computers to carry out diagnostics or perform software upgrades.

More than half of Danish shipping companies hit by cyber-crime

16th January 2018
By Grace Johansson- SCMedia

A survey by the shipping association of the CEO panel comprising of 26 senior executives revealed that the majority of Danish shipping companies - 69 percent - had been hit by cyber-crime according to a report in Seatrade Maritime News (SMN).

Consequently 69 percent of Danish shipowners have increased their IT budgets this year - an exact correlation with those who have been hit.

Mike Loginov CISO at Powel AS Norway, and president of IOTSA told SC Media UK that in the United States alone, the US$ 700 billion (£509 billion) shipping industry is expected to be valued at US$ 1.3 trillion (£900 billion) by 2023, and with the level of growth it's hardly a surprise that the shipping industry is of interest to the adversarial community.

He went on tell SC that "it also depends on which adversarial lens we focus on. If, for example, we consider the scenarios from a cyber-warfare perspective, the capability to seriously distrust the global supply and logistics chain makes cyber-attacks on shipping a strategic and attractive attack vector from a national defence position.

He adds: "As older ships with legacy technologies are replaced or refitted with modern interconnected capabilities they potentially become more vulnerable to direct cyber-attacks. Shipping companies should take the lessons learned to date very seriously to ensure that the risk is appropriately managed and mitigated. The integration of IT and OT systems through the growth of IoT use in the shipping and logistics world remains fertile ground for the inquisitive hacker and nation state players alike. Unless the industry takes serious steps to bolster its cyber-defence then the disruption the Danish shipping sector has experienced is likely to become much more prevalent as tensions between nations increases."

REFERENCES

MARINE CASUALTIES		
ARTICLE	SOURCE	PHOTO SOURCE
Sanchi sank	https://worldmaritimenews.com/archives/240598/burning-oil-tanker-sanchi-sinks-off-china/ https://www.reuters.com/article/us-china-shipping-accident/black-box-for-sunken-tanker-sanchi-opened-iranian-media-idUSKBN1FD0SX https://www.reuters.com/article/us-china-shipping-spill/how-sanchis-spill-could-spread-idUSKBN1FF1AK (https://www.ecowatch.com/oil-spill-east-china-sea-2526611780.html https://www.japantimes.co.jp/news/2018/02/02/national/tokyo-takes-steps-deal-sanchi-oil-spill/#.WnhdEXIL-Hyo https://www.nature.com/articles/d41586-018-00976-9 https://news.nationalgeographic.com/2018/01/iranian-oil-spill-china-environment-spd/	http://rooselaw.co.uk/RoosePartners%20Casualty%20Newsletter%20-%20Edition%20252%20-%2024%20January%202018.pdf http://gcaptain.com/japan-sees-little-chance-oil-slick-sunk-tanker-reaching-coast/ http://metro.co.uk/2018/01/15/sanchi-oil-spill-worse-exxon-valdez-tanker-sinks-off-coast-7230827/
Qi Cheng Xian Feng sank	https://www.shipwrecklog.com/log/2017/12/qi-cheng-xian-feng/qi-cheng-xian-feng-1/	https://www.shipwrecklog.com/log/2017/12/qi-cheng-xian-feng/qi-cheng-xian-feng-1/
“Genessa” fire	http://rooselaw.co.uk/RoosePartners%20Casualty%20Newsletter%20-%20Edition%20252%20-%2024%20January%202018.pdf https://insurancemarinenews.com/insurance-marine-news/genessa-blaze-extinguished/	
Kenekuai Sank	https://worldmaritimenews.com/archives/237825/indonesian-cargo-ship-sinks/	http://seanews.co.uk/cargo-vessel-carrying-cement-sinks-in-indonesia/

PIRACY REPORTS

ARTICLE	SOURCE	PHOTO SOURCE
Containership attacked in Port Harcourt	http://rooselaw.co.uk/RoosePartners%20Casualty%20Newsletter%20-%20Edition%20239%20-%2025%20October%202017.pdf	http://rooselaw.co.uk/RoosePartners%20Casualty%20Newsletter%20-%20Edition%20252%20-%2024%20January%202018.pdf
Bulk Carrier attacked in Bony	http://rooselaw.co.uk/RoosePartners%20Casualty%20Newsletter%20-%20Edition%20242%20-%2015%20November%202017.pdf	
Pirates target crude oil tanker off Nigeria	http://worldmaritimenews.com/archives/234180/pirates-target-crude-oil-tanker-off-nigeria/	
Tanker released after 6 day hijack	https://www.safety4sea.com/pirates-release-abducted-tanker-all-crew-safe/	
Second vessel disappears in Benin within a month	http://www.bbc.co.uk/news/world-africa-42938518 https://news.sky.com/story/search-launched-for-missing-oil-tanker-feared-hijacked-by-pirates-11237632	https://news.sky.com/story/search-launched-for-missing-oil-tanker-feared-hijacked-by-pirates-11237632

CYBER REPORTS

ARTICLE	SOURCE	PHOTO SOURCE
Cyber-attack alert weeks before USS John S McCain warship crashed	https://www.thetimes.co.uk/article/cyber-attack-alert-weeks-before-uss-john-s-mccain-warship-crashed-3660dfsrr	
Computer hackers targeted BW Group	Tradewinds.com	
Israel naval dome demonstrates hack attack on ship's controls	https://insurancemarinenews.com/insurance-marine-news/israels-naval-dome-demonstrates-hack-attack-ships-controls/	
More than half of Danish shipping companies hit by cyber-crime	https://www.scmagazineuk.com/more-than-half-of-danish-shipping-companies-hit-by-cyber-crime/article/737074/	

Contacts

For more questions should you wish to contribute to a future edition please contact:

Mike Ingham

T: +44 (0)20 7204 1864

E: Mike_Ingham@ajg.com

Haris Lagios

T: +44 (0)20 7204 6211

E: Haris_Lagios@ajg.com

Notes


NO SMOKING
NO SMOKING

Gallagher

The Walbrook Building
25 Walbrook
London
EC4N 8AW

T: +44 (0) 20 7204 6000
F: +44 (0) 20 7204 6001

GST-210976408

Gallagher

Insurance | Risk Management | Consulting