www.bunkerspot.com Volume 17 Number 2 April/May 2020

BUNKERSPOT

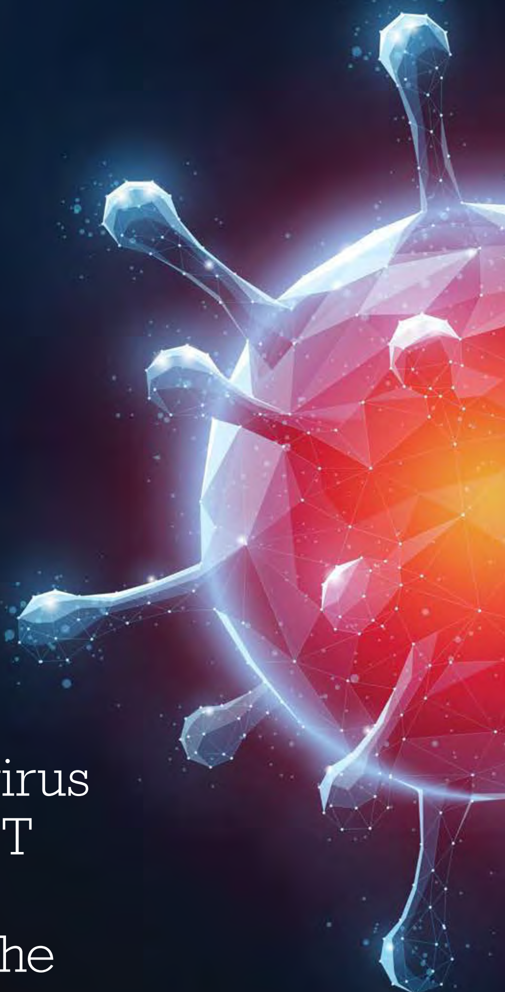
FUELLING THE FLEET

KEEPING THE US NAVY ON THE MOVE

INSIDE:

LNG AND METHANE SLIP
IMO 2020: FUEL UPDATE
FOCUS ON ST PETERSBURG
CORONAVIRUS GUIDANCE

Unseen enemy



'Going viral' describes the rapid spread of disease, as seen with the current coronavirus outbreak, and has also been coined by the IT sector to describe computer cyberattacks. **Steve Simms** of Simms Showers considers the cyber security challenges facing the bunker sector

In 2017, World Health Organization experts wrote that '[f]ew doubt that major epidemics and pandemics will strike again, and few would argue that the world is adequately prepared.'[1] The COVID-19 spread once again brings vivid awareness of the profound human and economic costs of being unprepared.

Also in 2017, the International Maritime Organization's (IMO) Maritime Safety Committee adopted its Resolution MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems. By no later than 'the first annual verification after 1 January 2021 of company Documents of Compliance, flag States (Administration) must 'ensure that cyber risks are appropriately addressed in safety management systems.'[2]

At the time of writing, the COVID-19 'Coronavirus' pandemic and nearly world-wide Internet connection have combined to have more people working remotely than any time in history.

This remote working extends to many in the bunker industry. However, the bunker industry has relied on computerised operations for years, in pace with the larger maritime industry's increased computerised and Internet reliance. The 2018 Guidelines on Cyber Security Onboard Ships[3] details that:

> Ships are increasingly using systems that rely on digitisation, digitalisation, integration, and automation, which call for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet. This brings the greater risk of unauthorised access or malicious attacks to ships' systems and networks.

As the IMO's 1 January 2021 date requiring safety management systems to 'appropriately address' cyber nears, the dual phenomena of the COVID-19 pandemic and intense industry Internet reliance highlight the need for bunker providers to prepare now for unprecedented cyber risk, and provide important lessons about how to be prepared.

THE NEW VIRAL REALITY

There have been other viral pandemics during the past 20 years: SARS (2002–03), bird flu/H5N1 (2003–07), Swine flu/H1N1 (2009), MERS-CoV (2012–present and Ebola (2013–16).[4] Now, however, international travel connects exponentially more people. Since 2003's SARS pandemic, the number of air travellers has more than doubled. So, an expert observes about COVID-19 that 'we're getting numbers faster, but that's partly because there are more numbers.... It's a real disease on the move.'[5]

More people now since 2003 are connected on the Internet: growing from about 9.3% of the world population in 2003 to 58.7% in January, 2020.[6] There are 11 new Internet users each second. One million more people use the Internet daily, with the average user spending more than 6 hours a day online.[7] Just as more human connections may have more quickly brought on COVID-19, more Internet connections likely will bring on more challenges to cybersecurity.

> '1981 brought the first computer virus; now the average annual cost of data breaches worldwide exceeds $2.1 trillion. Data breaches deposed about 4.5 billion records during the first part of 2018 alone; 2019 saw the theft of 2.7 billion identity records, posted on the Internet for sale'

1981 brought the first computer virus; now the average annual cost of data breaches worldwide exceeds $2.1 trillion. Data breaches deposed about 4.5 billion records during the first part of 2018 alone; 2019 saw the theft of 2.7 billion identity records, posted on the Internet for sale.[8]

The maritime industry generally, and the bunkering industry in particular, has been directly affected by this. One of the most public incidents was in 2013, after a World Fuel Services (WFS) trader received an emailed quote request from a thief misrepresenting himself to be a Defense Logistics Agency (DLA) employee. The DLA is the U.S. government fuel supplier and a regular WFS customer. The email exchanges continued and WFS contracted with the thief for over $17 million of marine gasoil (MGO). Then, off the coast of Lome, Togo, a bunker tanker transferred the MGO to another ship, which then disappeared with the fuel. Only after the DLA didn't pay WFS' invoice, did WFS learn that it had been a cyber fraud victim.[9]

Also well publicised was when A.P. Møller-Maersk, on 17 June 2017, fell victim to the 'Not Petya' virus – which originated, cyber security experts believe, as a part of Russia's cyber war against Ukraine. Maersk's staffers watched as their laptops began to show 'messages in red and black lettering. Some read 'repairing file system on C', with a stark warning not to turn off the computer. Others, more surreally, read 'oops, your important files are encrypted' and demanded a payment of $300 worth of bitcoin to decrypt them."[10] The attack affected Maersk for days, endangering the operations of its 800+ vessels, which, at the time, represented nearly a fifth of international world shipping capacity. It erased vessel manifests, and brought terminal gate operations to a halt. Maersk personnel had to compensate using paper, Excel spreadsheets and Whatsapp. Maersk began to recover in about two weeks. '[In the wake of NotPetya, [Maersk] IT staffers say that practically every security feature they've asked for has been almost immediately approved. Multifactor authentication has been rolled out across the company, along with a long-delayed upgrade to Windows 10,' said one commentator.[11]

Maersk's public estimate was that the attack cost it $200-$300 million but privately, it may have been more. At the same time, those depending on Maersk's systems, such as trucking and logistics companies, also lost millions of dollars.

Of course, these are only two of the most publicised cases of marine industry – and bunker industry in particular – cyber fraud. The author receives reports regularly of less publicised 'cyber fraud' but, for the size of loss to the particular bunker supplier, significant and embarrassing. A particularly increasing situation is where email communications are intercepted, the customer receives a spoofed email with 'new' wire instructions to send payment to the thief, and the bunker supplier either goes unpaid or the customer pays twice.

Vessel and bunker providers' systems involve the use of both computerised information technology (IT) and operational technology (OT). IT is communication of facts and data, OT is what makes systems work. As the WFS and Maersk examples show, cyber security problems can affect both IT and OT with expensive and dangerous results. Cyber breaches can affect essential bridge navigation systems like GPS, and ballast water, vessel stability, and engine systems. They can also affect bunkering systems such as mass flow meters and electronic quality measurement devices. The bunker industry also relies to a remarkable extent on emails transmitting imaged copy of stems, paper bunker delivery notes and invoices, all of which easily can be infected with viruses.

The COVID-19 phenomenon of course parallels the introduction of a computer virus which quickly can proliferate from a bunker supplier to a customer. Just as greater human interaction more quickly proliferated the COVID-19 virus, so also does more Internet use more quickly proliferate cyber security issues.

What that means is that safety management systems addressing cybersecurity – which might have been 'appropriate' years ago – will not be so now, or compliant with IMO Resolution MSC.428(98) after 1 January 2021.

With the intense focus now on stopping the COVID-19 viral pandemic, what lessons can it show (oddly, but then again, not so much) for Resolution MSC.428(98) compliance – and importantly, for bunker suppliers assisting their customers to achieve, and maintain compliance?

FLATTENING THE [CYBER] CURVE

The U.S. Centers for Disease Control and Prevention (CDC) has published a series of guidelines to stop the COVID-19 spread.[12] They can relate as directly to achieving today's 'appropriate' cyber security.

CDC Guideline 1: Know How it Spreads

There is currently no vaccine to prevent coronavirus disease 2019 (COVID-19).

The best way to prevent illness is to avoid being exposed to this virus.

The virus is thought to spread mainly from person-to-person.

Between people who are in close contact with one another (within about 6 feet).

A Document of Compliance (DOC) is a flag state's confirmation that a document holder complies with the requirements of the International Management Code for the Safe Operation of Ships and for Pollution Prevention (the ISM Code). The 'Company' is 'the owner of the ship or any other organisation or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the shipowner and who on assuming such responsibility has agreed to take over all the duties and responsibilities imposed by the ISM Code.'[13]

Although bunker providers (unless they also operate bunker tankers) are not required to have DOCs, the safety management systems that the ISM code requires must include bunkering operations. Compliance therefore must include bunker providers' work with their customers, who must comply with the ISM code and its cyber security requirements effective from 1 January, 2021. Customer systems must include detailed procedures about how crew work with bunker providers to enable bunkering. Safe bunkering management systems require detailed communication, monitoring, planning, and execution with bunker providers and customers working together to manage the range of risks inherent in bunkering. Consequently, on and after 1 January 2021, bunker providers must have 'appropriately addressed' cyber risks, so that their customers can reflect those in their Document of Compliance.'

'In the bunkering industry there are more and more frequent email spoofs seeming to originate from customers, with attachments which once opened, release viruses, worms or other malware into systems'

The question for bunker providers then is, how might our operations increase customers' and our cyber risk? Also, how do our customers' operations increase our cyber risk?

One area is the use of removable media. Flash drives and other media, introduced among vessel and other systems, can transmit computer viruses. The 2018 Guidelines on Cyber Security Onboard Ships[14] highlight an incident, relating to a 'Bunker surveyor's access to a ship's administrative network':

> A dry bulk ship in port had just completed bunkering operations. The bunker surveyor boarded the ship and requested permission to access a computer in the engine control room to print documents for signature. The surveyor inserted a USB drive into the computer and unwittingly introduced malware onto the ship's administrative network. The malware went undetected until a cyber assessment was conducted on the ship later, and after the crew had reported a 'computer issue' affecting the business networks. This emphasises the need for procedures to prevent or restrict the use of USB devices onboard, including those belonging to visitors.

Consequently, electronic data transfer rather than removable media transfer is best, although far from perfect. That is, email and attachments may be virused. In the bunkering industry there are more and more frequent email spoofs seeming to originate from customers, with attachments which once opened, release viruses, worms or other malware into systems. Vessels frequently may be running old software without systems to detect outgoing viruses, and the same may be true for bunker suppliers dealing with traders, or vice versa. Consequently, bunker providers must have effective, current systems for virus removal from attachments, and ideally, systems which do away with attachments – at least scanned ones – altogether.

The most scanned document is a bunker delivery note, almost always completed on paper and then scanned and delivered by attachment. Leading bunker traders now are finally seriously considering digital bunker delivery note systems, which employ effective encryption against malware. Another benefit of these systems is that they minimise human contact and therefore transmission of 'real' viruses. A good rule of thumb: the more humans, or computers, which must touch a piece of paper, or data, the more chances of viral transmission, computer, or human.

Above all, though, remember that at the centre of every cyber security problem is human error. It can be the simple error of not picking up the phone to verify wire instructions, or of clicking on an attachment not passed through an effective malware detection and removal program, or using old and easily hacked software. Just as a central way to stop COVID-19 spread is to limit close contact, good cyber security means always expecting that there will be malware transmission, and so keeping ahead of that by prevention. Good 'distance' prevents greater problems.

CDC Guideline 2: Take steps to protect yourself

Clean your hands often

Avoid touching your eyes, nose, and mouth with unwashed hands.

One essential protection is to evaluate your computer systems, both IT and OT, and their potential vulnerabilities. Then, make sure that you employ systems which regularly scan for viruses, and, that your systems employ limitations of points of contact with other systems, such as those of vessels, customers or suppliers.

To comply with IMO Resolution MSC.428(98), many vessel operators will use the Oil Companies International Marine Forum (OCIMF), Tanker Management Self-Assessment (TMSA), 7th Edition (VIQ7) Vessel inspection Questionnaire[15], or something similar to it. Its section on cyber security asks a number of questions, including the following:

> 7.14 Are Cyber Security Policy and Procedures part of the Safety Management System and is there a Cyber Response Plan onboard?
>
> Note: Do the procedures include a risk assessment of issues such as:
>
> - Threats such as from malware; phishing attacks etc.
> - Identification and protection of vulnerable systems (Electronic Chart Display and Information Systems (ECDIS), etc.)
> - Mitigation measures, (USB control, etc.)
> - Identify key personnel within the company (including who the master reports suspected incidents to)
> - Hard copy of key contacts (e.g. Designated Person Ashore; Company Security Officer, etc.)
> - Password management/record?
> - Contractor compliance

Note: Does the Cyber Response plan contain guidance on:

- What 'symptoms' to look for,
- Immediate actions to be taken and
- Name, position, phone number and email for the Responsible Person to be contacted

7.15 Are the crew aware of the company policy on the control of physical access to all shipboard IT/OT systems?

Note: Inspectors should observe if access to USB ports on 'Shipboard IT/OT' terminals are controlled (i.e. there are measures in place to block/lock USB/RJ-45 ports on these terminals. Procedures should include the protection of Critical equipment such as ECDIS from malware and virus attacks. Procedures should include the control of access to all shipboard IT/OT terminals including access to Servers which should be in a secure location. The procedures should also include access by any third-party contractors and technicians.

7.16 Does the company have a policy or guidance on the use of personal devices onboard?

Personal devices include phone/tablets etc and storage devices such as USB sticks.

Check if the policy is implemented by both, crew and visitors, e.g. all third-party contractors and technicians.

7.17 Is Cyber Security awareness actively promoted by the company and onboard?

Note: Active promotion might include:

- 'Cyber Awareness Material' displayed by all IT terminals and in crew rest rooms
- Training films shown to crew
- Crew specific training
- Instruction on safeguarding of passwords
- Responsible use of social media
- Policy on the use of personal devices and its inclusion in shipboard joining familiarisation checklists
- May include companies own employee/contractor Authorised User Policy (AUP) agreements
- Company certified as per ISO 27001.

Bunker providers would do well to evaluate their cyber security procedures, with questions similar to the above which apply to their own operations. The answers respond directly to taking steps to protect yourself' with specific, identified and regular procedures, akin for cybersecurity as washing hands regularly, and not touching with unwashed hands, is for avoiding COVID-19.

CDC Guideline 3: Avoid close contact

Avoid close contact with people who are sick

What enforcement of IMO Resolution MSC.428(98) should do, with robust enforcement, is to identify vessels which are non-compliant. Theoretically, those vessels, which must be inspected yearly to receive their Document of Compliance and thus be permitted to operate, and which cannot 'ensure that cyber risks are appropriately addressed in safety management systems,' will not, after 1 January 2021 be re-documented.

So, an obvious way to avoid close contact with vessels which are 'sick' with cyber risk, is to observe which are issued with Documents of Compliance after 1 January, 2021. There is, however, no similar documentation system for bunker providers, however.

'The most scanned document is a bunker delivery note, almost always completed on paper and then scanned and delivered by attachment. Leading bunker traders now are finally seriously considering digital bunker delivery note systems, which employ effective encryption against malware'

Focusing on vessel compliance, however, once must consider that enforcing compliance with IMO Resolution MSC.428(98) will require an even further degree of capability of flag State authorities. Inspecting the vessel systems, crewing requirements, and even bunker sulphur content compliance and enforcing the law and regulation applying to those is one thing, but enforcing the 'appropriate' addressing of cyber risk is a new area of enforcement. Interestingly enough, IMO Resolution MSC.428(98) is a dynamic requirement. That is, compliance is different with Resolution MSC.428(98); what is 'appropriate' for some flag states might be too exacting for others. Or, on the other hand, what may be 'appropriate' for an inspection at one time, might be inadequate – with an outbreak of malware – for another. This presents enforcement challenges which are different than for other IMO standards, measurable by certain numbers.

One characteristic of COVID-19 has been that many carry it without obvious symptoms. The presumption from this is that many more are infected than manifest the virus, and even those going on to manifest symptoms do not show those for 14 or more days. The virus also may continue to be active in the air for hours, or on surfaces for days.

So, again the best approach is to presume that all other cyber systems that one may contact, are cyber security risks. Distance, that is, placing layers of security around entrance and exit-ways to IT and OT systems, is always better than close contact. As with this Guideline for COVID-19, the way to 'appropriately address' cyber risks, is to keep distance with security measures that examine and remove incoming and outgoing risks.

CDC Guideline 4: Stay home if you're sick

Maersk, infected with NotPetya, followed this Guideline. It was inconvenient. But Maersk disconnected all of its external outgoing and incoming contacts, until it could diagnose and remove the problem. In other words, Maersk self-quarantined.

Even with the best preparation and security, bunker providers and their customers still may experience a cyber security issue. The best approach is to disconnect, contact those who might have received the malware or other problem from your system, and not connect until the infection is gone.

Not doing this can raise not only customer problems, and continued internal problems but also legal problems, as Uber (the call-hailing service) learned from the United States Federal Trade Commission (FTC). The FTC is a U.S. Government agency with authority to prosecute 'unfair methods of competition'[16], which include cybersecurity breaches.[17] In 2014, an Uber engineer mistakenly posted an access key on a public code-sharing site. A hacker used the key to steal the personal data about more than 100,000 people. The FTC learned of this and began prosecution, but during the prosecution, in 2016, Uber experienced an even worse cybersecurity breach (25.6 million names and email addresses, 22.1 million names and mobile phone numbers, and 607,000 names and driver license numbers of U.S. Uber riders and drivers) due to, basically, the same lax security that Uber had in 2014. Uber did not react to the 2014 problem, or disclose the 2016 problem to the FTC. The FTC imposed stringent controls on Uber, which will require Uber to submit to direct FTC oversight for years.

CDC Guideline 5: Clean and disinfect

Clean AND disinfect frequently touched surfaces daily.

To paraphrase this final Guideline: 'Stay ahead of the problem.'

Just as COVID-19 is spreading to what seems to be unexpected places, as Internet use continues to grow and vessel operations have even more 'cyber' aspects, one must stay ahead of situations by 'cleaning and disinfecting' often, particularly, those frequently-used parts of computer operations.

For example, protections against malware, including anti-viral software, must be kept up to date, anticipating ever-increasing cyber security challenges. There should be scheduled audits of cyber security systems, because, again (continuing to keep in mind the IMO Resolution MSC.428(98) requirements), what may be today an 'appropriate' way to 'ensure that cyber risks are... addressed' probably will not be adequate or 'appropriate' six months from now.

In tandem with the issue of MSC.428(98), the IMO's Maritime Safety and Facilitation Committees in 2017 published Guidelines on Maritime Cyber Risk Management[18] The Guidelines emphasise that:

> Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitisation, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

To keep 'cleaning and disinfecting', the Guidelines give the common sense recommendation that "[r]eference should be made to the most current version of any guidance or standards utilised."

Just like 'cleaning and disinfecting', 'frequently' is common sense, so is keeping up with 'appropriate' cyber security. Exercising 'common sense' depends on keeping up with good information. The Guidelines recommend the 'Guidelines on Cyber Security Onboard Ship's, discussed above.

The bunkering industry works regularly with ISO standards, and so there also is a further standard to become familiar with: 2 ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. The ISO 27001 series gives best practice recommendations on information cyber security management.[19] One can expect that flag authorities will look to ISO standards to determine whether a safety management system's cyber security is 'adequate'.

A further, recent resource is the February, 2020 Digital Container Shipping Association's (DCSA) publication offering cyber security guidance, specifically preparing for Resolution MSC.428(98) compliance.[20] The DCSA offers the guidance to other sectors of the maritime industry, in addition to container carriers, to prompt MSC.428(98) compliance.

Overall, however, the best preparation should be undertaken along with advisors – legal and technical – who keep up with the standards and also can provide a neutral, and exacting, third party evaluation.

It's like paying someone to come in to clean your house (or, having an honest friend who will tell you that your house needs cleaning). That is, somehow that person always sees the cobwebs you don't or should know of a better way to clean, because, after all, that's what they do, while you sell bunkers.

1 January 2021, just like the 1 January 2020 0.50% sulphur content deadline, is arbitrary. That is, it is, of course, not anticipating a major maritime cybersecurity attack on 2 January.

What is certain, however, is that just as there has been with COVID-19 and the pandemics before it, there will be more pandemics, and more cyber security challenges. The maritime industry generally, and the bunker industry, will experience increasing and increasingly sophisticated cyber security challenges, as Internet use multiplies, just as COVID-19 multiplied because of presently increased world-wide human interaction.

The focus on COVID-19 response, and 'flattening the curve' – along with the compelled use now of remote systems – is an ideal time to consider in a very personal way the common sense of MSC.428(98) compliance, and steps to take now to more than 'appropriately' address and maintain that.

[1] V. Fan, D. Jamison and L. Summers, *Pandemic risk: how large are the expected losses?*, Bulletin of the World Health Organisation, 2018;96:129-134. doi.

[2] Maritime Cyber Risk Management In Safety Management Systems; see also, IMO, Maritime Cyber Risk.

[3] The Guidelines (Version 3, 2018) were produced by maritime industry organizations Produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and the World Shipping Counsel, copy at a number of sources including.

[4] Rebecca Onion, *We've Had a Lot of Pandemics Lately. Have We Learned Anything From Them?*, Slate, January 3, 2020.

[5] Ed Yong, The New Coronavirus Is a Truly Modern Epidemic, The Atlantic, Feb. 3, 2020, quoting Tom Inglesby, a health-security expert at Johns Hopkins Bloomberg School of Public.

[6] Internet World Stats, *Usage and Population Statistics*

[7] Jeannie Dougherty, Internet growth + usage stats 2019: Time online, devices, users, ClikZ, May 1, 2019

[8] *List of data breaches.*

[9] The opinion of the United States District Court, Southern District of New York in *AGCS Marine Ins. Co. v. World Fuel Servs.*, 187 F. Supp. 3d 428; 2016 U.S. Dist. LEXIS 65119 (S.D.N.Y., May 17, 2016) describes the fraud. The Court held that WFS' insurance carrier was required to cover WFS for the fraud.

[10] Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired, Aug, 22, 2018.

[11] Greenberg, *The Untold Story,* id.

[12] Centers for Disease Control and Prevention, Coronavirus Disease 2019 (COVID-19), *How to Protect Yourself.*

[13] IMO Resolution A. 788(19) adopted on 23 November 1995, *Guidelines on Implementation of the International Safety Management (ISM) Code* by Administrations, A 19/Res. 788.

[14] Guidelines (Version 3, 2018), *id.* at 31.

[15] TMSA, © Copyright OCIMF 2019.

[16] 15 U.S. Code § 45, "Unfair methods of competition unlawful; prevention by Commission."

[17] *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 256-57 (3d Cir. 2015) (inadequate cybersecurity controls by hotel provider Wyndham, leading to theft of thousands of customer credit card numbers and other identifying information).

[18] MSC-FAL.1/Circ.3, 5 July 2017.

[19] ISO Standards are available for purchase at https://www.iso.org/obp/ui/#home. For a description of the ISO 27001 series, see https://en.wikipedia.org/wiki/ISO/IEC_27000-series#Published_standards

[20] Cyber Security Implementation Guide download page and Guide.

J. Stephen ('Steve') Simms is a principal of Simms Showers, LLP, a US-based law firm representing leading bunker suppliers and traders world-wide.

Simms Showers advises bunker suppliers and traders on credit security, recovery, sales terms and conditions and MARPOL-related issues, including those in this article, for 2020, 2021 and beyond.

Steve Simms serves as Chair of the International Bunker Industry Association (IBIA) Legal Working Group and is a past IBIA Board member. The opinions and recommendations of this article are his and not necessarily also those of IBIA, except if identified specifically as such.

Tel: +1 443 290 8704
Mob: +1 410 365 6131
Email: jssimms@simmsshowers. com
Web: www.simmsshowers.com