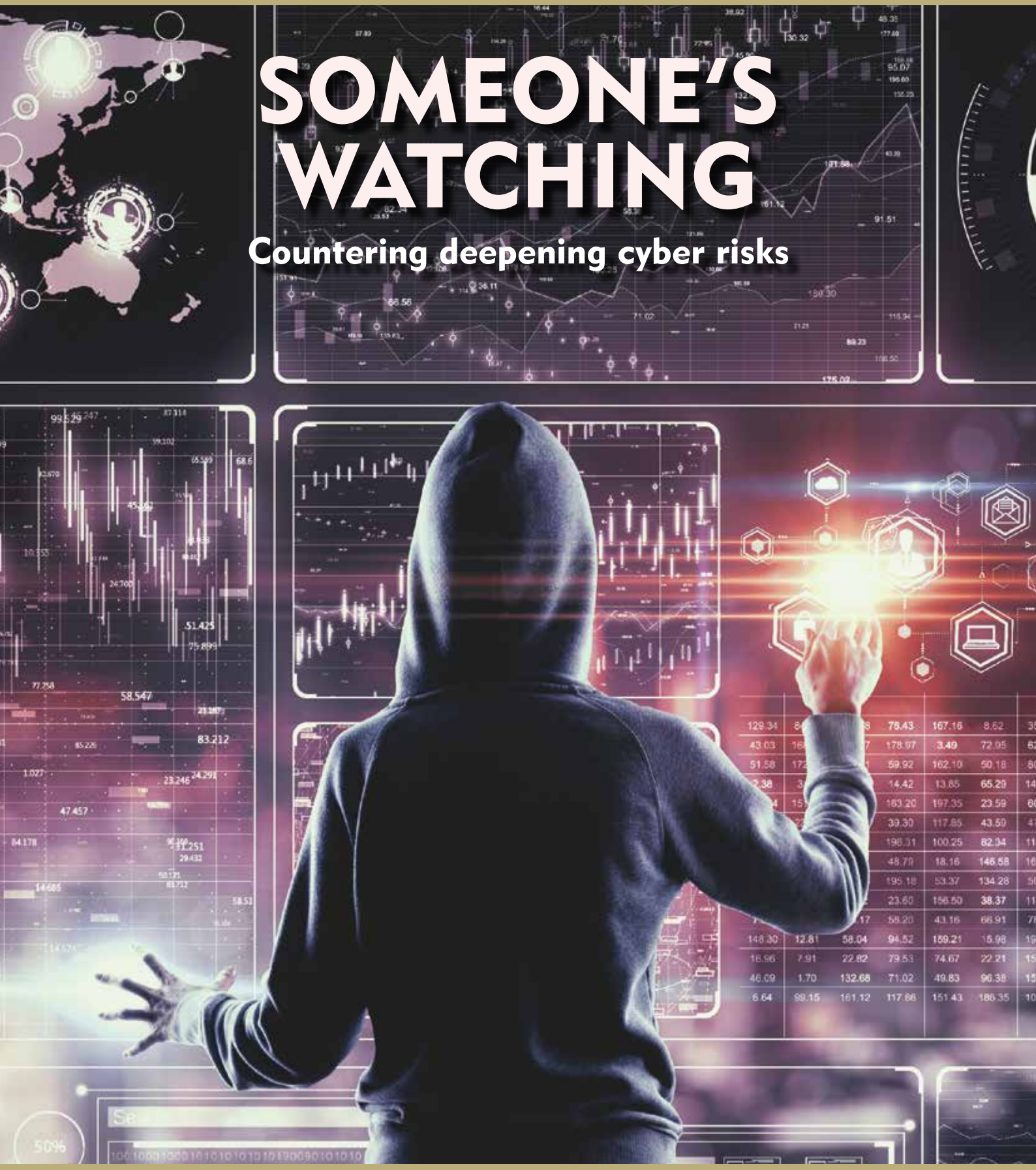
SHIPPING Network
The official magazine of the Institute of Chartered Shipbrokers
ROYAL CHARTER Centenary 1920-2020
Promoting professionalism in the shipping industry worldwide
Issue 67 December 2021

SOMEONE'S WATCHING

Countering deepening cyber risks



Class shortfalls | Insurance exclusions | Port guidelines | Risk management

Get your message to the right audience

Advertise with Shipping Network to reach over 4,000 named individuals and companies. Our high pass on rate means that each quarterly issue is viewed by over 16,000 people.

Shipping Network's readership is truly global and covers the full breadth of the professional shipping services sector, including Ship Managers, Ship Owners, Agents, Freight Forwarders, Brokers, Charterers and Traders.

Take advantage of competitive and transparent advertising rates:

GBP£1,000 full page A4 in the run of the magazine

GBP£500 half page A5 in the run of the magazine

GBP£1,500 full page A4 inside back or outside back

To book space for your advertising message, contact Matt Gilbert:
+44 (0)20 7357 9722, m.gilbert@ics.org.uk.

Don't delay – there is a strict limit to the number of positions available in each issue and once they are gone, they are gone!

Setting and surpassing exacting standards

Glenn Murphy outlines his goals for the Institute over his tenure as international chairman

Glenn Murphy

I am extremely honoured to have been elected to the role of chairman of this revered institution.

Somebody once said that with great power comes great responsibility which is by no means lost on me as I embark on this role. The power and control of the Institute is vested, not in one single person, but in all of Controlling Council on behalf of the membership and as such, it is our collective responsibility to see that we deliver on that crucial undertaking. The organisation recently came through some very challenging times which wasn't the result of one single bad decision or event but a culmination of elements over time. It is clearly our duty, as your elected Board members, to make sure that this doesn't happen again and that we put measures in place that safeguard the Institute for future generations.

While we are clearly in a better position now than we were 12 months ago, it would be unwise to think that there are no further challenges ahead

As Executive Council (Exco, the Institute's Board), we have spent much of the last two years in particular focusing on improving our financial and corporate governance. I am certain that valuable lessons have been learnt and consequently important decisions have been taken in a thoughtful and decisive way. Our work at Exco has been aided by the exemplary contribution of the members of the Finance & Audit Committee and the Governance Working Group. The addition of robust financial and better governance frameworks shall provide us with far more solid foundations to build on with our future organisational plans and goals. While we are clearly in a better position now than we were 12 months ago, it would be unwise to think that there are no further challenges ahead.

In the coming months my immediate priorities will be in three areas. First is the Executive Board/Council. During the last two years the Board has been confronted with many challenges that none of us would have expected or wanted but which have been dealt with in a professional manner. As an Institute, we set the highest standards for our students and Members. As chairman, I will challenge the Board that we continue to set the same exacting standards for ourselves and our committees in executing our delegated mandate.

Second is the business of the Institute. It is important in our oversight role as a Board that we ensure that we make decisions which give clear strategic direction, in particular in the core areas of membership and education. We need to make sure that we prioritise the investment of our time, capital and resources in alignment with our values and principles to maximise the return for our membership. We, as a Board, shall continue to monitor and consider other opportunities or strategic investments that add value to our membership, enhance brand value and provide a worthwhile return on our time and resources. It is essential that we make sure that the Institute's organisational structure and capabilities are appropriate for implementing the agreed work programmes and objectives. I have prioritised this particular area for my first meeting as chairman of the Executive Council.

Third is communications and brand value. I see this as being central to having a more connected and joined up Institute of the future. The last two years of being isolated in and out of lockdowns has challenged us to find alternative ways to communicate as branches but also in our own daily professional lives. We have seen really brilliant initiatives at local and regional levels that have promoted the work of the Institute and connected members, students and branches together in new ways not used before. Communications and promotion of the Institute's brand values isn't just a one-way or even a two-way street between the secretariat and branches but should be something that we use to connect the entire membership of the Institute. Shipping Network is an excellent internal communications tool, but we also need to continue to increase the profile of our work through the use of other external media, social and digital platforms. Replacing our current website – which is outdated – is something that needs to be addressed in the near future.

I plan to speak with all branch chairs, committee chairs and Controlling Council representatives in the initial weeks of my term. In particular, I would like to hear about their future plans and priorities at branch and committee level and how we can align these with the central planning through the Board with the secretariat.

I have already had some good discussions with our director, Robert Hill, in terms of future planning for the work of the secretariat and Board. Robert and his team have the confidence and support of the Board and I look forward to working with them in the future.

I also welcome Luis Bernat in taking up his new role as vice chairman and in joining myself and the president Kevin Shakesheff as the Institute's senior officers. I would also like to take the opportunity to thank Lord Mountevans as immediate past president who was a fantastic support to me during his term. Also, sincere thanks to Susan Oatway as outgoing chairman for her time and in particular her dedication to the Institute over the past two years.

I will do my utmost to serve the interests of the Members and progress our pursuit to ensure the Institute remains a relevant and progressive professional body in global shipping. ***SN***

Glenn Murphy FICS
Chairman

Stealth mode for cyber threats

As I write this, two deeply worrying cyber-related articles have caught my eye. The first – *'Cybercrime underground flush with shipping companies' credentials'*, from Intel 471 – reveals that shipping company data is already out there and being sold on cybercrime networks. That means for many the damage has been done, networks have been compromised and vulnerabilities have been exploited. It is no longer a case of keeping the wolves from the door; they are in, and they are ready to cause business-crippling havoc.

The second article – *'Greek shipowners cyber tricked over Halloween weekend'*, courtesy of *Splash247.com* – lays bare just how vulnerable the industry is to cyber-attacks. "Multiple" Greek shipping companies were hit by a ransomware attack that spread through the systems of IT consulting firm, Danaos Management Consultants, in early November.

Here, it's the route to access that makes me uneasy. While the cyber risks presented by third-party remote maintenance for operational technology are known, less is being done to counter attacks through a third party's software on shoreside systems. As one cyber specialist in our feature on *Page 17* aptly observes, hackers are currently ahead of shipping operators.

We hear on a regular basis of the big companies that have been hacked, but this will be just the tip of the iceberg. Cyber-attacks are real – and given the current activity on the cybercrime underground, your company could already have been a victim. **SN**

Carly Fields, FICS
Editor

Key contacts

Editor of *Shipping Network*: Carly Fields FICS

Institute of Chartered Shipbrokers
30 Park Street, London, SE1 9EQ, UK

Telephone: + 44 (0) 20 7357 9722
Fax: + 44 (0) 20 7357 6348
Email enquiries: membership@ics.org.uk
For advertising enquiries please contact the Editor on: editor@ics.org.uk

Shipping Network is the official publication of the Institute of Chartered Shipbrokers.

The views expressed in *Shipping Network* are not those of the Institute of Chartered Shipbrokers, their directors or their officers unless expressly stated to be such.

The Institute of Chartered Shipbrokers disclaims any responsibility for the advertisements contained in this publication and has no legal responsibility to deal with them.

Shipping's play in a high-stake game

Cyber protections need to be set, strengthened and regularly surveyed, finds Felicity Landon

Felicity Landon

Yesterday was your lucky day! An email arrived, congratulating you on winning $1 million. Did you click on the link to claim the money? "I am pretty sure that ten years ago, some people would have clicked that link. Today, most people would not," says Capt Sanjeev Verma. In that respect, perhaps we have moved forward when it comes to cyber security – but the clear consensus is, the shipping industry has a long way to go, and the stakes are getting ever higher.

Topic: Cyber

Keywords: Risks, people, protection

Background: Shipping companies are not doing enough to fill gaping cyber vulnerabilities

There have been plenty of high-profile warnings: Maersk Line was crippled by a Petya cyberattack in 2017, while in 2020, CMA CGM was hit by a ransomware attack and MSC suffered a malware attack which brought down its customer-facing websites for several days.

And yet, shipping companies that suffer any kind of hack are often reluctant to share information, fearing their reputation will suffer. Consequently, many companies are not learning the lessons they should, says Capt Verma, who is managing director of Landbridge Ship Management and a Member of the Institute's Hong Kong Branch.

He asks, how many people know what exactly went wrong in the headline cases? Mostly they just know something went wrong.

"Sharing information is not very easy and companies are reluctant to do so. In the banking industry, they do share information – but in the shipping industry, there is still far to go. Companies are naturally worried about reputation in discussing details."

Many shipping companies will never learn the lesson "unless it happens to them", says Capt Verma. Companies need to focus on their own cybersecurity – but they also need to talk to each other about the risks.

Growing risks

As the shipping industry becomes ever more digitalised and automated, so the targets for would-be hackers proliferate and the risks intensify.

The awareness is there, he says: "For every shipping company, if cyber is not at the top of the agenda it is in the top two or three." However, he says, hire in a very junior hacker and they will likely find loopholes which they can easily exploit by creating a couple of phishing emails. "The question is, are shipping companies doing what they ought to fill in the gaps? In general, no."

Cyber should be at the top of every shipping company agenda

A key reason, he says, is that a shipping company's interest most of the time is how to earn money, rather than how to spend it. "Money coming into your account is no problem – the problem is when it is going from your account."

And here, shipping's legendary pride in being a 'people' industry based on personal relationships could even add to the risks. "Maybe they think 'I do not have to do a lot of due diligence because the person is known to me'". But personal relationships are of no consequence if a hacker manages to change a G to a Q in a familiar email address and submit a routine looking invoice. Someone then glances at the details and doesn't see the change, and potentially millions are paid into an account set up by the scammer.

There is nothing like regulation to give companies the shove they need. The IMO's Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems entered into force at the beginning of 2021. It encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems, as defined in the International Safety Management (ISM) Code. Ship owners and operators must fulfil the requirements in time for the first annual DoC (Document of Compliance) audit on or after January 1, 2021.

Capt Verma says another reason for the increased focus on cybersecurity is social media and concerns about reputation.

"With the kind of presence companies now have on social media platforms, reputation is very important when it comes to providing service. Continuity of business is one of the biggest risks if hacked."

Getting back to business

Continuity has, of course, also been a challenge during Covid-19 and one solution – working from home – has added to the cyber risks, in terms of both vulnerability and impact. "Information

becomes paralysed if there is an attack on your system, stopping people doing business, so you lose the trust of partners – and in today's world, it will be in the news very quickly."

Getting business back on track as fast as possible is the most important priority after any kind of cyberattack, says Capt Subhangshu Dutt, chairman of the Institute's Singapore Branch.

He notes the difference in vulnerability between liner operators and other segments such as bulk carriers and tankers.

"Liner operators have to be considerably more digitalised and connected, because they have online booking, etc. Secondly, they are very linked up with agency offices all over the world. The direction is towards getting more digitalised and automated and accessible to customers – so yes, the likelihood of breaches and threats will increase. Accessibility for customers and terminals, offering digitalised services and links, means the risk is increasing. But there is no turning back. You have to keep going and try to make it as secure as possible."

However, he points out the challenge: "Considering the broad spectrum of people who need to access a company system, you have to have a user-friendly system – too many barriers, and the purpose is lost. The users are people, simply booking."

Keeping it "under the covers" after suffering a hack doesn't help at all, says Capt Dutt. "I think liner companies cannot avoid the release of this news into the media. Clients are the first ones that know – they want to book a container and see a blank screen. Sooner or later, it will come out."

London and South East Branch Member Mark Sutcliffe says that when a hack happens, the desire is to keep it under wraps to protect reputation.

However, he highlights research earlier this year by AMMITEC (the Association of Maritime Manager in Information Technology and Communications) into the cyber maturity and preparedness of shipping companies. A questionnaire was sent out to AMMITEC members – IT managers, CIOs and IT leaders in shipping companies. Of the 50 companies that answered, 76% of said they would be willing to anonymously report a security threat or incident to an AMMITEC controlled database, while 66% said they would be willing to anonymously report the key findings, remarks and recommendations from external cybersecurity audits or inspections of their vessels.

> "The hackers and criminals are exploring, probing, learning – I would say this is a honeymoon period before it gets more difficult"

Information sharing

Sutcliffe is director of the CSO Alliance, which brings together company security officers from around the world to share information on maritime security threats. He says: "Ships at sea have no one to report these incidents to but we need to know what's going on. Criminals don't see any national boundaries. Shipping companies need to know what these criminals are doing, why and when, and what is the impact. There is a desire to pull it all together."

He says the industry is beginning to do more to react to the cyber threats, but warns: "A million people visit the dark web every month and buy really good quality, highly effective ransomware equipment that is being deployed against all industries – healthcare, banking, police. We are just one industry and there is more money to made in others… at the moment.

"The industry hasn't been hammered as we know it will be in the years to come. The hackers and criminals are exploring, probing, learning – I would say this is a honeymoon period before it gets more difficult."

Fellow CSO director Simon Osborne adds that the paucity of information sharing means there isn't a clear picture of the threats shipping companies are facing. "Many companies are concerned about loss of navigation – we know it is possible for ships to have their navigation and controls taken over by hackers, but we will only know if it is occurring if ships are reporting these incidents."

People are a shipping company's biggest strength and biggest weakness

Learn to stand out with the Institute's Online Academy

Online courses available – enrol now!

Study package includes registration, all materials, live classes and exams

Call: +44 (0)20 7357 9722
or email: shipping-school@ics.org.uk for more information

INSTITUTE OF CHARTERED SHIPBROKERS

The spoofing of vessels' AIS (Automatic Identification System) tracks is a growing concern; SkyTruth analyst Bjorn Bergman recently wrote about identifying numerous false AIS tracks which seemed plausible but "could compromise vessel safety, decrease confidence in a crucial collision avoidance system and potentially spark international conflict".

Lost at sea

In an article entitled 'Are you where you think you are?', Uniteam Marine commented that the Global Positioning System (GPS), together with GLONASS, BeiDou and Galileo, forms the basis of the Global Navigation Satellite System (GNSS) that provides positioning, navigation and timing information via satellites orbiting above the Earth. This information allows anyone with a compatible receiver to determine their position, velocity and precise universal and local time.

In 40 years, this system has gone from "a highly classified and very expensive tool used only in military and space applications to something that almost anyone can have in their pocket via their mobile telephone".

It goes on to note: "There have been several recent cases of vessels reporting that their actual position is not the same as that shown by their satellite navigation system. In one widely reported incident in 2017, over 20 vessels in the Black Sea found that their GPS position showed that they were around 30 kilometres inland."

Sutcliffe says that when it comes to AIS falsification or hacking of navigation systems, "there hasn't been a stratospheric bad accident that can absolutely be laid on this issue."

However, it has been suggested that the detention of the tanker Stena Impero by Iran may have taken place after the vessel's navigation systems had been affected by spoofing, he said.

Information abounds

There is no shortage of advice on cybersecurity; for example, BIMCO's Guidelines on Cyber Security Onboard Ships, which sets out a cyber risk management approach to identify threats, identify vulnerabilities, assess risk exposure, develop protection and detection measures, establish response plans, and respond to and recover from cyber security incidents.

The Guidelines emphasise that cyber risk management should involve the senior management level of a company on an ongoing basis – not just the ship security officer or IT manager. It also stresses the need to focus on both IT (the systems managing data and support business functions) and OT (operational technology), the hardware and software that directly monitors or controls physical devices and processes, from engines to navigation systems. Are the OT systems and their working environment protected from unauthorised access and changes? Is there remote access to the OT systems and, if so, how is this monitored and protected?

Landbridge brought in Lloyd's Register's Nettitude to help it fulfil the cybersecurity requirements for its DoC. "The experts will go through a company's systems and procedures, try to find out where the gaps are, and start working on these, closing the loopholes – whether it is the system in the office or on ships, or the visibility of individual employees on a social media platform, everything is taken care of," says Capt Verma. "Certain ethical hacking methods are utilised to see if the system can be breached or taken control of remotely. Finally, certification is provided.

There have been several cases of vessels reporting that their actual position is not the same as that shown by their satellite navigation system

"There are unique challenges for any shipping business in the sense that the assets are floating on the water, where the bandwidth is still not very strong – it might still take hours to download something we do in seconds on our phones. In any other industry, everything is fixed – an office in Hong Kong, a branch in Singapore, and so on. But our 'offices' might be in the Indian Ocean today and the Atlantic tomorrow.

"The first thing IT experts encounter is that they are working on a system or asset where nothing is through wire but all through satellite. The shipping company needs to work with IT people who understand how the assets are connected, what systems are in place, and what equipment onboard could be hacked."

People power

Ultimately, shipping companies need to get the message across to their employees. "Educating your people about cybersecurity is the one thing that can really reduce the cyber risk," says Capt Verma. "Having an IT department is one of the corrective actions you can take but every cyber risk happens when an employee does something wrong – clicking boxes, opening the wrong site, turning off the antivirus because it takes too long to update something. We have arranged training for cybersecurity for our staff with a third party, as well as internally. Training people is one of the strongest tools the company can employ."

That's echoed by the CSO Alliance's Sutcliffe, who says: "Most of it is about your people – they are both your biggest strength and your biggest weakness. You need a budget to train them, to make them aware of what is going on – and you will get that investment back in spades. Really, what you are trying to do is create a human firewall, which will allow you to better protect your company."

You can't be certain things will never go wrong, he adds, but if you are prepared, with the processes and training in place, then if the flare goes up, you do not need to panic. "You can go into structured drills and procedures, understand the PR element, notify customers, etc. You can handle it so much better and get back on board quickly." ***SN***

Investing in the cyber offensive

AGCS' Capt Rahul Khanna explains why IT security should not be put on the backburner

Capt Rahul Khanna

In September 2021, CMA CGM was hit by a cyber-attack almost a year to the day after it had previously suffered a ransomware incident which affected much of its IT infrastructure. The latest attack saw the French container shipping major note that it had suffered a leak of data on "limited customer information" but that its IT teams had developed and installed security patches promptly.

Topic: Insurance

Keywords: Disruption, risk, cover

Background: While an uptake in cyber insurance is positive, the threat to ships continues to grow

The digital era may be opening up new possibilities for the maritime industry but its growing reliance on computers and software and increasing interconnectivity within the sector is also making it highly vulnerable to cyber-attacks.

The CMA CGM incident is the latest in a growing number to have impacted the shipping sector in recent years. All four of the largest shipping companies – Maersk, Cosco, MSC and CMA CGM – have been victims of cyber-attacks in recent years. Port operators have also been affected. Even the United Nations' global shipping regulator, the International Maritime Organization was recently targeted by a cyber-attack, forcing some of its services offline. In particular, ransomware has become a global problem.

> "Marine insurers have been warning for years about the cyber risk to shipping"

Ransonware surge

According to security services provider BlueVoyant, shipping and logistics firms experienced three times as many ransomware attacks last year as in 2019. A spike in malware, ransomware, and phishing emails during the pandemic helped drive a 400% increase in attempted cyber-attacks against shipping companies through the first months of 2020.

To date, most cyber incidents in the shipping industry have been shore-based, such as ransomware and malware attacks against shipping companies' and ports' database systems. But with the growing connectivity of shipping, the fact that geopolitical conflict is increasingly being played out in cyber space – recent years have seen a growing number of GPS spoofing incidents, particularly in the Middle East and China, which can cause vessels to believe they are in a different position than they actually are – and with the concept of autonomous shipping, there is little doubt that cyber risk will become a more important exposure that will require much more detailed risk assessment going forward.

At the same time, the crippling ransomware attack against the 9,000-kilometre-long Colonial oil pipeline in the US in May 2021 has raised concerns that critical maritime infrastructure could be increasingly targeted in future. The attack resulted in the pipeline's systems, which connect some 30 oil

CMA CGM has been hit twice by cyber-attacks in as many years

refineries and nearly 300 fuel distribution terminals, being forced offline, resulting in petrol shortages across the eastern US.

Growing awareness

Marine insurers have been warning for years about the cyber risk to shipping. From a hull perspective, the worst-case scenario is a terrorist attack or a nation state group targeting shipping in a bid to inflict damage or major disruption to trade, such as blocking a major shipping route or port. While this would seem a remote possibility, it is a scenario we need to understand and monitor. Although an accident, the recent blockage of the Suez Canal by the ultra-large vessel *Ever Given* is an eye-opener on many fronts as it shows the disruption a momentary loss of propulsion or steering failure on a vessel navigating a narrow waterway can cause.

The good news is that the shipping community has grown more alert to cyber risk over the past couple of years, in particular in the wake of the 2017 NotPetya malware attack that crippled ports, terminals and cargo handling operations. However, reporting of incidents is still uncommon as owners fear reputational risk and delays from investigations.

Meanwhile, cyber security regulation for ships and ports has been increasing. In January 2021, the International Maritime Organization's (IMO) Resolution MSC.428(98) came into effect, requiring cyber risks to be addressed in safety management systems. The EU's Network and Information Systems Directive also extends to ports and shipping. This is a step in the right direction but the problem at the moment is quite extensive. Despite these measures we have seen a sharp rise in attacks.

Cyber cover

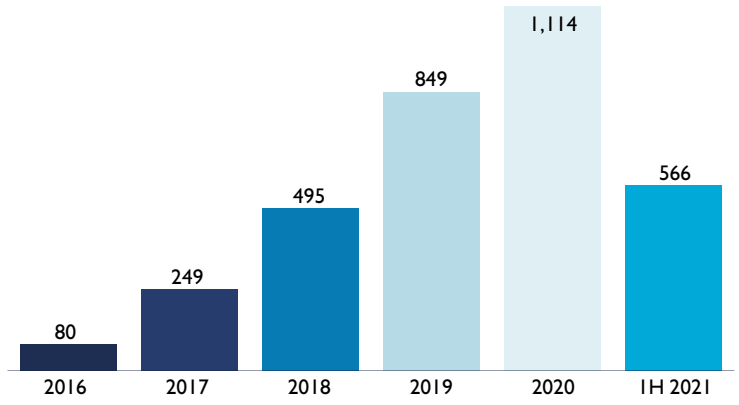
Increased awareness of – and regulation around – cyber risk is translating into an uptake of cyber insurance by shipping companies, although mostly for shore-based operations to date. Typically, marine hull insurance policies exclude coverage against cyber-attack or any loss arising from a malicious act involving the use of a computer system, given the potential loss accumulation issues from such scenarios. Instead, shippers have to purchase standalone cyber insurance coverage, but to date the readiness of many in the sector to buy a marine hull specific cyber cover has been limited.

However, the threat to vessels is growing as more and more ships are linked to onshore systems for navigation and performance management. Smart ships are coming, and we would expect demand for insurance to develop accordingly.

What we may see in the future is a potential increase in demand for a combination of onshore/offshore coverage and this is something we will need to discuss and observe with our clients and brokers to see how far this can be taken by marine hull insurance and how far it can be taken by a broader scope of cover in a combined policy.

Fortunately, there are also a growing number of resources available to help seafarers learn about common vulnerabilities. Just one example is the internationally recognised United States Maritime Resource Center, which assists the industry in cyber awareness, safety and security through evidence-based research. Then there are an increasing number of cyber security guidelines which can be followed, such as those from the IMO, but also from other important organisations such as BIMCO, CLIA, Intercargo and Intertanko.

Number of cyber-related claims per year*

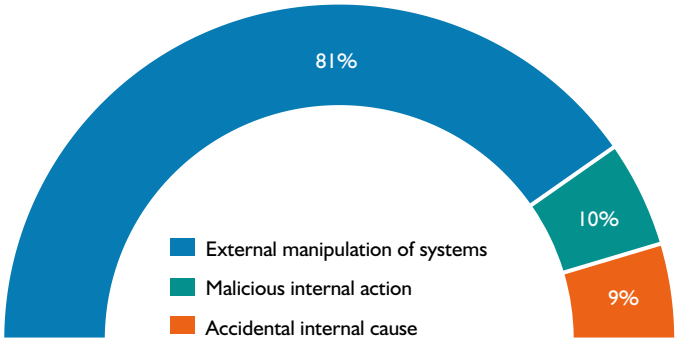


*Note: data refers to cyber claims across all lines of insurance business, not just marine

Source: Allianz Global Corporate & Specialty

Cause of loss by value of claims*

Based on the analysis of 2,916 claims worth €751mn (US$885mn) reported from 2015 until June 30 2021



*Note: data refers to cyber claims across all lines of insurance business, not just marine

Source: Allianz Global Corporate & Specialty

Standard practices

There are also standard practices that can be implemented to reduce cyber risk, such as defining personnel roles and responsibilities for cyber risk management and identifying the systems, assets and data that, when disrupted, pose risks to ship operations. Ship owners also need to implement risk control processes and contingency planning, developing and implementing activities necessary to quickly detect a cyber event. Identifying measures to back up and restore cyber systems impacted by a cyber event is obviously crucial.

Of course, these are challenging times for the shipping industry. However, IT security should not be put on the backburner. It is vital that investment in cyber risk education and security is not neglected at this time, despite economic pressures, as this risk has the potential to have catastrophic consequences, given the right confluence of events.

AGCS is working with our clients in assessing their cyber security preparedness. We strongly recommend clients to stress test their IT infrastructure against cyber threats and invest in mitigation measures. **SN**

Captain Rahul Khanna is global head of marine risk consulting at Allianz Global Corporate & Specialty, www.agcs.allianz.com.

Ship protection goes deeper than expected

ABS' John Jorgensen explains why a systematic approach is key to creating a ship security program

John Jorgensen

It seems that every day brings new reports of cybersecurity incidents and breaches, new vulnerabilities, risk pronouncements, and warnings. In the marine industry, we greet these articles and notices with the understanding that cybersecurity affects us, but sometimes it is decidedly unclear how we can proceed in such a complicated area that affects so much of our lives.

Topic: Class

Keywords: Control, security, notation

Background: Cybersecurity notations help companies and crews understand, maintain, and safely operate onboard automation systems

Cybersecurity is relevant to all fields that use digitally connected automation systems. With computer screens and controls in nearly every space on the ship, we can too easily dismiss cyber affairs as 'something the IT people have to do'. But in reality, we are most concerned about the impact of cybersecurity on asset management and business function reliability.

To that end, consider what systems or apparatus the ship has installed that may be considered cyber-relevant (in other words devices or systems with microprocessors, programmable devices and software). These include, but are not limited to, navigation and radar, power management, vessel management, engine performance, ballast water management, dynamic positioning, heating and air conditioning, refrigeration, cargo elevators and deck cargo cranes. A typical, relatively modern ship may have between twenty and forty automated systems onboard.

Once we recognise that a significant number of onboard systems are capable of digital communications and are highly connected to shore-side monitoring capabilities, we also realise that these systems affect nearly every function aboard the ship. That makes the notion that IT personnel are solely responsible for protecting cyber-enabled systems an open question: if the functional systems aboard ship, whether networked or standalone, are helping the whole crew perform their duties, doesn't protection of the ship's operations and business functions become part of the entire crew's responsibilities?

Ship security program is key

Better organisation of complicated sets of tasks allows people to understand them, as the tasks can be turned into categories that are merely complex. The key is to make tasks and routines as simple as possible so as to turn them into normal parts of the ship or company culture.

Protecting ship systems must be part of the company and crew culture

The ship's systems will commonly include information technologies (IT) and operational technologies (OT). IT is the basis for computers and communications around the ship, OT is the foundation for cyber-physical functions that allow computerised systems (navigation, propulsion etc) to fulfil ship operational and security needs.

OT includes programmable logic controllers, distributed control systems, and human-machine interfaces; some OT devices are connected to IT systems, while others are only connected to other OT systems. Because of this IT/OT connectivity, the different skills required to manage interconnected IT and OT systems, effective communications and cooperation between the two groups are essential.

A useful way to address the installed technology systems onboard the ship is with a dedicated security program. Such programs are already required by the International Maritime Organization (IMO) under the International Ship and Port Facility Security Code, which governs physical security. With the IMO's 2021 requirements to include cybersecurity in the ship's Safety Management System, it becomes worthwhile to consider how a company and crew can satisfy cybersecurity requirements efficiently and effectively.

Establishing a standard

A company's security program revolves around standards that, when tailored for the company and the ship, become both necessary and sufficient to satisfy the security needs of onboard crew, systems, and functions. This balance between 'enough security' and minimum disturbance to business processes requires knowledge of the ship's operational systems and onboard business processes.

The standard by which the program is established and executed is a key factor for the crew. Protecting ship systems must be part of the company and crew culture, not additional

or tasks assigned outside normal shipboard duties. To that end, a cybersecurity method can be a primary enabling factor to bringing cybersecurity into the ship's operations and systems, while minimising the burden of cyber-related tasks and responsibilities.

Considering that automated systems and automation grow each year, the crew's relationship to systems and ship functions in secure and safe ways is important to all. That's where a classification society notation enters the discussion as a standard to which a vessel is built and operated.

In an automation-heavy environment, the class notation for cybersecurity will provide a clear execution framework for establishing and maintaining the ship's cyber program. There are several factors critical to its success: what to do, how well it's working, and what else is needed.

What do we have to do? The cybersecurity notation provides a guide for program execution. Processes support the program, giving the crew a set of activities that bring completeness to the security program, with measures for progress.

How are we doing? The notation provides a ready checklist of operational activities and procedures that can be self-assessed or self-audited.

What else should we consider? Self-assessment allows crew and company to understand their current risks and their posture in controlling those risks to people, systems, ship, and environment.

Notation examples

ABS offers several cybersecurity notations that aid a company and crew in understanding, maintaining, and safely operating their automation systems. These include 'CS-System' which provides a way for shipbuilders to install and integrate systems provided by original equipment manufacturers with systems that are certified for cybersecurity, providing documentation to integrators and owners for secure integration and safe operations. 'CS-Ready' provides a method that guides the shipyard in preparing a newbuilding for delivery to the owner, with appropriate documentation of systems, configurations, and safeguards in place.

CS-1 (and the CS-2 for larger fleets and more digitally complex vessels) is the notation for operational ships or offshore assets that provides guidance for implementing a sustainable and continuing cybersecurity program for fully operational vessels. CS-1 implements the IMO 2021 requirements as an integral part of its security functions.

ABS CyberSafety notations are built around eight activities which define the entire program, and to which all selected security controls are linked. The activities are

1. A security program is established, with a manager designated.

2. Policies and procedures integrate cyber and physical security processes for governing automated systems processes, operations, and safety.

3. An incident response team is designated and trained, and a response plan for automated systems is available.

4. Systems inventories and diagrams (topologies) are made and kept current.

5. Risk assessment is performed on a regular basis.

6. A risk management system is used in conjunction with the SMS.

Ships' systems include information technologies and operational technologies – both susceptible to cyber attack

"In an automation-heavy environment, the class notation for cybersecurity will provide a clear execution framework for establishing and maintaining the ship's cyber program"

7. Training for crew and company personnel on ship systems and policies is performed regularly, results recorded, and maintained.

8. Management of change is a critical program that governs all automation systems and crew interfaces with systems.

These items are the keys to a cybersecurity program. The notation provides the program framework, into which security controls from cyber frameworks like the NIST Cybersecurity Framework (CSF), ISO 27000, and others may be introduced.

Security controls are business rules that, when put into place, will govern or allow/limit use of systems and functions. Controls selected for implementation in a company or on a ship require someone to be in charge of implementation and response procedures if something goes wrong, understanding of the risk if the control(s) is not functioning correctly, regular management of security and risk, specific security procedures training for crew and configuration and patch management.

Any framework of security controls can be integrated into a company's program if it is structured to support security and safety of the systems based on a competent risk assessment and management plan.

Class notations for cybersecurity provide a present and powerful execution framework for security in the shipboard environment. The chosen security controls work within the cybersecurity program put into place within the notation's guidance. The guidance calls for organising and structuring the program to work for the crew as a workable process for safety, security and reliability of automation systems. **SN**

John Jorgensen is chief scientist and director of cyber security at ABS, www.eagle.org.

Even newbuild ships tested by PenTestPartners haven't proved compliant with the IMO's cyber requirements

Black hole of class compliance

PenTestPartners' Andrew Tierney urges caution in accepting a ship as cyber compliant

Ship's classification societies have a key role to play in the International Maritime Organization's cyber security requirements: MSC-FAL.1/Circ.3 – Guidelines on maritime cyber risk management and Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems.

Based on our experience, there are some significant issues coming that maritime insurers need to be aware of before writing cover for any vessel that includes direct cyber or indirect interruption or loss as a result of a cyber incident.

Topic: Regulation

Keywords: Classification, compliance, confusion

Background: Class societies are mistakenly trying to fit cyber into their normal way of working

Currently, classification societies are short on the skills to accurately assess the cyber risk of a vessel.

We've tested the security of more than 50 vessels. None of them, even one fresh out of the yard, would come close to being compliant with MSC.428(98). Yet, multiple classification societies are publicly announcing that they have certified vessels as cyber compliant.

Why the disconnect?

The challenge for classification societies is getting assessors that have the right level of cyber skill and giving them the tools and processes to uncover security risks. At the moment, there is lack of understanding of ships' IT & OT systems.

One of the main issues is the reliance on paper and design reviews rather than having assessors investigating and understanding the systems and networks onboard. The skills and knowledge used during a survey of physical equipment and processes are very different to those required to audit a network. A simple example that sums it up well is: if the classification society auditor hasn't connected a laptop to the networks on the vessel, it's unlikely that they have done a thorough job.

Insurers are going to be burned in the future, writing a maritime cyber policy and setting premium based on a classification society survey, then subsequently being presented with a claim for cyber business interruption or worse as the result of a hack.

One would expect the underwriter to launch a case against the classification society for negligence or malpractice, but case history around incidents such as the spill involving the Prestige indicate a significant challenge to establishing liability.

Why the problem?

Classification society surveys have traditionally been about the physical: lifeboats, fire alarms and other safety systems. Are they present, do they work, are they safe and are records correct? The challenge is how to fit 'cyber' into that way of working.

While rare, cyber incidents on board affecting ship systems are increasing. An incident that prevents a vessel sailing, or jeopardises its safety is increasingly possible. Most of the

incidents to date have been untargeted, often ransomware impacting corporate machines or ECDIS. A targeted attack by a hacker with knowledge of maritime technology could easily cripple a ship. We should know, we've done it, at the request of the operator obviously!

The potential impact of a cyber incident is significant, particularly if targeted. Control of propulsion systems remotely, including Azipods; control of generator controllers – potentially leading to remote and repeated blackouts; access to the loading computer remotely – allowing crucial stability calculations to be altered; disabling of all fire detection systems and the VDR – both of which can be considered detainable deficiencies, particularly for large passenger vessels.

You name it, if it's tech on a vessel, we've had control of it during a penetration test, usually remotely. It can take a lot of effort and knowledge to take control of a system remotely – especially without being detected. From an attacker's perspective, it may be easier – and more damaging – to permanently disable or "brick" systems.

Why is vessel cyber so difficult?

Paper designs for vessel networks rarely equate with the reality, even fresh out of the yard. Much effort is put in to designing segregated and secured networks on board, yet when implemented many of these segregations are compromised for operational, practical or other reasons. All too often, the maritime technology supplier doesn't follow the design, or circumvents security controls simply to get a system working.

In one case we found that all devices on board had certificate-based network authentication, or NAC – an excellent security design. However, any device that didn't have a certificate was placed in to a virtual 'tar pit' for unauthorised devices.

The unintended consequence of this was that all unauthorised devices could communicate with each other within the tar pit. Along comes a provider who doesn't want to route dedicated cables through already sealed deck penetrations, down nine decks from the bridge to engine room. They found they could plug their devices into any network port, get assigned to the tar pit, and everything worked.

The result? Anyone who plugged any device in to any port on the vessel could take control of the main engines. That would not show up on any check-list based survey.

Time erodes cyber security in many ways:

1) Operations defeat segregation. Ships' engineers make changes to systems, sometimes to fix problems, sometimes to make remote administration easier. Their primary goal is to keep systems operational. These changes can break down the careful network segregation from initial designs.

2) New vulnerabilities are found over time. Applying updates is not part of the culture in maritime systems – "if it ain't broke don't fix it" is a popular mantra. As new vulnerabilities are found, patches are eventually released by the technology vendor. It they aren't applied, the system remains vulnerable, yet hackers now know about the vulnerability so security gets worse.

3) Reused passwords are exposed. Password reuse is commonplace, so passwords for accounts are increasingly exposed from other sources. It's not unusual for us to find that a vendor uses the same password across every vessel they have installed their systems on.

Much is made by the maritime technology industry of IEC 62443 and the latest integrated bridge systems are starting to show signs of cyber-awareness at vendors. However, there is so much more to this.

We find new vulnerabilities in shipping technology most weeks. Typically, these will have been present in vessel systems for years and by some fluke have not been exploited to date, perhaps because of the degree of skill required to find them and there is 'easier prey' on land. As other industries improve their security, shipping comes into the firing line for hackers.

Simply releasing a new product that's written with security in mind isn't enough. What about vessels running older unsupported versions of your software that are full of security holes? Those 'holes' aren't usually the customer's fault – they're the vendor's fault. So, does the vendor have an obligation to provide improved software?

The next major problem for maritime tech vendors is to learn to accept security reports from researchers in good faith and act upon them. It's hard to receive perceived criticism from third parties who aren't your customers, but it's essential you do if your security is to improve.

Ensure someone at the business is tasked with receiving, triaging and managing security vulnerability reports, but more importantly is empowered to effect change in your organisation.

We often find technology on board that has been created with security in mind, but the 'cyber' message hasn't filtered down to the installers who fit and commission the equipment in the yard. All the vendor's efforts are undone by an under-resourced installer who is rushing to make sure the vessel returns to service in time. 'Get it working' is not enough anymore.

'Cyber' is a minefield for shipping. It is also a minefield for insurers. Classification societies currently have limited cyber risk assessment skills, but they are getting better. Vessels are already being classified as 'cyber' compliant when they really shouldn't be. Tread very carefully when writing a shipping cyber policy. Get external advice. **SN**

Andrew Tierney is a consultant for PenTestPartners. This article first appeared on the PenTestPartners website and is reproduced with their kind permission. For more information go to www.pentestpartners.com.

ECDIS have been the target of most at-sea ransomware incidents to-date

Quash cyber fear with information sharing

NORMA's Lars Benjamin Vold explains why better data sharing is needed to mitigate risks

Lars Benjamin Vold

Cyber security has been a hot topic for many years within the shipping and maritime sector. The shore side part of the sector – as with many other industries – has gone through years of extensive digitalisation. We now also see that different digital solutions are being developed and implemented at high speed for vessels, such as systems for remote access, remote control, and autonomous operations. But with these solutions, new vulnerabilities are also introduced.

Topic: Resilience

Keywords: Data, intelligence, insight

Background: Establishing a data-based knowledge resource will give shipping a fighting chance at overcoming cyber risk

NORMA's team corroborate multiple sources and use proven intelligence methodology to analyse data and information

The International Maritime Organization resolution on cyber security, which came into play from January 1, 2021, has raised the minimum level of requirements for ship operators. Nonetheless, we still see that many shipping companies are struggling with how to address cyber risks effectively.

First, it is challenging to identify the risks, to grasp the potential consequences and to implement effective measures which have real risk-reducing effect. At the same time, many leaders are struggling to fully understand cyber risks and it is difficult to know where to start and where to stop mitigation work since many of the solutions are very costly. It doesn't help that there are many different actors speculating widely on how vessels may be affected by digital attacks. Several commercial actors use fear as a marketing method – they often claim to also have the single miracle cure to solve it all.

Land-based focus

So, what have we at the Norwegian Maritime Cyber Resilience Centre (NORMA) seen since our establishment on January 1, 2020? During the first ten months of operations, the intelligence and information sharing team at NORMA have followed the cyber situation closely and received data and information from members, partners, and different providers and through monitoring the deep and dark web and malware repositories. NORMA's four-person team corroborate multiple sources and use proven intelligence methodology to analyse data and information. Based on this the team provides decision support through reports and advisories to members which can be implemented in their risk management processes. Since the establishment of the centre, we have also had a response service where we have assisted members in handling several cyber incidents.

The incidents we have handled, and those reported by external sources, have almost exclusively been directed towards land-based IT-infrastructure. Two types of incidents stand out, ransomware and invoice fraud. Ransomware can be particularly painful to counter as the threat actors continue to develop their tactics and often delete backups, encrypt data, and threaten to leak sensitive information online.

When it comes to invoice fraud, many incidents start with what is called Business Email Compromise (BEC). This is where the threat actor takes control of email accounts and inserts themself into an existing conversation to alter bank details. The attacks are technically unsophisticated, but we have seen examples of threat actors being extremely good at impersonating real emails and that show high-level insight into the industry.

Mission critical

What about attacks towards critical vessel systems? As previously mentioned, many are discussing the possibility of critical vessel systems being hacked, and the consequences that might ensue. As of today, we have not observed any attacks targeting critical vessel Industrial Control Systems (ICS). We have seen incidents of vessel IT systems being affected by ransomware, and even Electronical Chart Display and Information Systems (ECDIS) being affected, but so far nothing has affected the systems controlling steering, propulsion, or other critical vessel systems. GPS or other GNSS systems have also been affected by spoofing and disruption campaigns, but the best mitigation measure for this is good seamanship. We have not seen reports of severe consequences of such interference.

Does this mean that the potential consequence of a vessel system being hacked are small? Certainly not. And we know that if a vessel loses steering or propulsion in a critical situation, the consequence for personnel, the environment and assets might


To date, NORMA has released 30 Vulnerability Notifications addressing different vulnerable equipment used onboard vessels

"Ransomware can be particularly painful to counter as the threat actors continue to develop their tactics and often delete backups, encrypt data, and threaten to leak sensitive information online"

be devastating. We also know that many ICS systems onboard vessels are vulnerable to attacks as old and outdated systems often are utilised. The preferred security measure for such systems has so far been to isolate them. To date, we have released 30 Vulnerability Notifications to our members addressing different vulnerable ICS equipment used onboard vessels. It is obvious that as more vessel ICS systems are made accessible remotely or from the internet, and as threat actors adopt to the new situation, security must be addressed properly. This work should be based on knowledge and verified data and information.

Our work ahead

In addition to the work we are doing on intelligence sharing and response services, we have also established forums, both digital and physical, where members can share experience and best practice.

In June we launched our monitoring and detection service where we perform security monitoring of systems and detect threats in real time. This is now implemented with four shipowners, with more than 80 vessels and 3,000 land-based staff. We also have an active project where we perform the same security monitoring for ICS systems onboard vessels. As more of our members implement this service, we are increasingly capable of assessing data across several fleets allowing us to deliver unique insight into actual threats and vulnerabilities which can be fed back to members through our intelligence.

But above all, the most important aspect of NORMA is to establish the right knowledge base for further work. With seven (and soon to become nine) full time employees we aim to be a leading hub for operational maritime cyber security so that our members can base their decisions on real time data, knowledge, and insight. **SN**

Lars Benjamin Vold is managing director of the Norwegian Maritime Cyber Resilience Centre (NORMA). The centre provides cyber security services for the Norwegian maritime sector and operates on not-for-profit basis. More than 60 shipowners and operators have become members, representing more than 1,400 vessels. NORMA is a joint initiative between The Norwegian Shipowners' Mutual War Risks Insurance Association (DNK) and the Norwegian Shipowners' Association.

Call for mandatory US cyber measures

US politicians have called for mandatory cybersecurity measures for the transport and logistics sector in response to an increase in ransomware and other cyber-attacks.

At a hearing of the House Committee on Homeland Security in October, democrat Yvette Clarke said that the lessons learned from the hack of the Colonial Pipeline – resulting in 5,500 miles of pipeline being shut down – need to be acted on.

Senator Clarke said that it is now known that attackers infiltrated Colonial Pipeline's business network using a legacy VPN that did not require multi-factor authentication; the flow of information between Colonial Pipeline, the Cybersecurity and Infrastructure Security Agency, and the Transportation Security Administration (TSA) was slow, fuelled in part by ongoing confusion about which agency was in charge; and despite repeated offers from TSA, Colonial Pipeline had not yet undergone an important security assessment – a Validated Architecture Design Review – and did not have a disaster response plan that contemplated the full scope of cyber threats.

"Shocked by what we learned during their oversight of Colonial Pipeline and other recent high-profile cyber incidents, Members of Congress have begun to question whether the Federal government's approach to cybersecurity – which relies primarily on voluntary partnerships – actually works, or whether some security requirements ought to be mandated," she said.

Transportation and Maritime Security Subcommittee chairwoman Bonnie Watson Coleman added that higher security standards should apply to "all transportation modes", especially with the growth in connected and autonomous vehicles. And she said that the US Coastguard needs to enforce cybersecurity standards within ferries, ports, and maritime systems. **SN**

Shipping is taking a long, hard look at its cyber protections

Just another risk that needs to be managed

Carly Fields hears how it is possible for shipping companies to 'get their arms around' cyber risk

Carly Fields

Cyber is always all over us and the biggest threat to the whole industry, but it is just another risk that shipping needs to manage.

That was the assertion of AP Moller Maersk head of claims, Claes Westman in a panel discussion on cyber, technology and terrorism risk, hosted by Ince as part of London International Shipping Week.

Topic: Risk

Keywords: Attacks, protection, defence

Background: Shipping has made its cyber 'house' stronger, but hacks are evolving to find new vulnerabilities

And while shipping's defences against cyber-attacks have improved, there is still much more to be done. Rick Tiene, vice president of Mission Secure, used the analogy of a house to illustrate the scale of the problem: "We have made our IT house stronger and tougher. But while we have a better deadbolt, the garage is wide open." This is leading to more hacks on the operational technology front, which is the easiest and the greatest point of impact.

The human element is well publicised as the most common way for penetration, but more and more hackers are finding different ways they can get in. BIMCO head of maritime safety and security, Jakob Paaske Larsen pinpointed state sponsored actors as the most serious risk currently facing shipping, as their goals go beyond simple commercial gain. "This is growing and we have seen more attacks from state-sponsored hackers," he said.

Regulations are getting tighter around cyber protection in shipping, forcing companies to take a long, hard look at their cyber protections. One of the most significant changes has been the compulsory application of the International Maritime Organization's cyber guidelines as of January 1, 2021. "That means that all owners will have cyber on their risk registers and undertake legislation against those risks," said Astaara chief executive Robert Dorey.

There is still confusion lingering over whether a particular cyber risk is covered or not, but Larsen reminded shipping

Rich shipping pickings of cybercrime underground

The cybercrime underground is said to be 'flush' with shipping companies' credentials, according to Intel 471, a cyber threat intelligence service.

Over the third quarter of 2021, Intel 471 observed network access brokers selling credentials or other forms of access to shipping and logistics companies on the cybercrime underground. The shipping companies in question operate air, ground and maritime cargo transport on several continents and are responsible for moving billions of dollars' worth of goods around the world, Intel 471 said.

In an example, the firm said that within the span of two weeks in July 2021, one new actor and one well-known access broker claimed to have access to a network owned by a Japanese container transportation and shipping company. The new actor included the company's credentials in a dump of approximately 50 companies, allegedly all obtained via compromised Citrix, Cisco, virtual private network (VPN) and/or remote desktop protocol accounts. The well-known actor claimed to have access to several accounts belonging to the company, but did not reveal how they were obtained.

In September 2021, Intel 471 added, an actor with ties to the FiveHands ransomware group claimed access to hundreds of companies, including a UK-based logistics company. Intel 471 said it is most likely that access was obtained through a SonicWall vulnerability, given that FiveHands is known to use that access to launch its ransomware attacks. Additionally in September, a new actor claimed to have gained access to a Bangladesh-based shipping and logistics company through a vulnerability in the PulseSecure VPN.

"The world has previously seen the economic damage that can come from a cyber-attack on the shipping and logistics industry," said Intel 471.

"At a time when this sector is struggling to keep things operating, a successful attack could bring this industry to a screeching halt, resulting in unforeseen dire consequences for every part of the consumer economy. It's extremely beneficial that security teams in the shipping industry monitor and track adversaries, their tools and malicious behaviour to stop attacks from these criminals." **SN**

companies that this is a journey, not a destination. "We are definitely going in the right direction, but we will never be 'there'," he said. "This is not a destination. This is a journey and we will need to continually develop." Big incidents have "spooked" the industry, he added, and led to thorough reviews of cyber processes. "There is for sure an increased interest. I think the industry has learnt a lot and is on the right path."

Share and learn

Better information sharing could really shift the cyber protection needle. Mission Secure's lead cyber evangelist and ethical hacker, Weston Hecker urged shipping companies to share and learn from best practices as these can lead to safer and more secure environments. "Employee training and just information in general is a good way to stay on top of these things," he said.

This can help overcome the thousands of attempted attacks that a company the size of AP Moller Maersk fields every day. That level is something that Maersk "lives with", said Westman. These encompass everything from normal phishing emails to employees, to direct hacker attacks against Maersk's complete system.

Some shipping companies, however, have failed to appreciate that hacking has evolved. Today, it is less about a back-and-forth hacking process and more about a payload, said Tiene. "It's not like the old movies where someone hacks with cool hackers; in the modern world a hacker takes weeks or months planning an attack." While some attempted hacks might be "goofballs" just throwing something out there and hoping it will stick, others will be probing yet no attack has taken place. He said that means that for many, the moment a hack is discovered, it is already too late. "You need to stop the attack from embedding," he said.

"This is not a destination. This is a journey and we will need to continually develop"

Tiene advised companies to stop thinking of cyber as something to add to infrastructure: "We need to think of it as the infrastructure. It should be bedded in new and retrofitted."

'Low hanging fruit'

With 95% of cyber claims a result of human error, training is the low hanging fruit. On a ship, Astaara's Dorey explained that the crew are a good line of defence: "You can't manage everything, but on a ship with 18 pairs of eyes they are not going to give up, they will keep going and they will have had cyber drills."

That said, Tiene described ships with programmable controllers as in the "worst possible sweet spot". "They have evolved to be vulnerable to a hacker," he said. "They are not sophisticated enough to run their own cyber protection." This is a very risk-heavy area in terms of operational technology as currently hackers are ahead operators.

And the current downturn could exacerbate risks. Mission Secure's Hecker noted that less jobs are open in programming fields at the moment and those that can't find jobs end up writing malware. "It doesn't take a nation state to take down a company, it takes a 12-year-old with a computer."

But at the end of the day, everyone is capable of "getting their arms around the risk" and managing it, said Dorey. Westman agreed: "This is part of what we are doing today, it is nothing separate and I think this is how insurance should look at it as well. It has been part of what we are doing for the past two decades."

Larsen advised companies to stick to the guidelines and make sure risks are properly managed. Also, recognise that it is not possible to avoid all cyber incidents. And operators should look at a whole suite of cyber protection, not only practical solutions. Commercial mitigation can also be incorporated, for example through insurance and/or charterparty protection, he said.

While it is impossible to have 'zero risk' shipping, it is the industry's job to reduce any risk – including cyber – to an acceptable level, concluded Capt Michael P Elwert, moderator for the panel, senior maritime industry advisor and former chief operating officer for V.Ships Global Ship Management. **SN**

The art to working out your weak spots

Cyber's Owl's Richard Wagner and Daniel Ng ask how prepared your business is to respond to a cyber-attack

Daniel Ng

Richard Wagner

Something interesting happens when you lock a group of senior shipping executives in a room and put them through a cyber-attack drill. Given how unfamiliar cyber risk management is in shipping, the scenario quickly descends into guesswork based on false assumptions. It doesn't take them long to realise just how unprepared they are to make the necessary decisions to contain and recover. And in some cases, they are not even sure who in their organisation has the right information and is expected to take responsibility. Not a great place to be in.

Topic: Drills

Keywords: Testing, containment, recovery

Background: Regular cyber drills could end up being shipping companies most important line of defence, mitigation and containment

Earlier this month, CyberOwl alongside HFW, Navigate Response, and The Standard Club hosted a cyber security drill at the British High Commission in Singapore. This in-person event drew together senior business leaders across the maritime industry. The drill immersed participants in a cyber incident so they could feel the effects of the decisions they would have to make, and the preparedness of their company plans.

The following are the five key takeaways from the business leaders in the room.

Number 1, most shipping companies are not set up to get the right information to the right individuals at the right time.

Broadly, you can split up a cyber incident timeline into four phases:

- Phase 1: before you know you've been attacked.
- Phase 2: the point you find out.
- Phase 3: your first few hours of response.
- Phase 4: after the incident is contained.

Most people, not just the senior business leaders, obsess about Phase 3. It's easy to see why – many imagine cyber incidents to be like physical incidents e.g. a fire. So attention and obsession immediately turns to how rapidly their teams and crew can put out that fire.

One interesting takeaway from the exercise is that most of the business leaders weren't clear that their teams would even know the shipboard systems were under attack, until it was too late. There was little confidence that detection or monitoring systems were in place to flag up such alerts. So the obsession about putting in place a rapid response capability is somewhat misplaced, as there was no way of triggering that capability.

"To survive a cyber incident, what you need to do is help your team think on their feet. This is where regular drills are helpful"

First focus

There was also debate about what information was really important in the first few hours of response. Many instinctively wanted to know the nature of the attack – is it malware? Is there a ransom note? Who is trying to attack us? What are the attackers demanding? While these are good questions, the focus in the first few hours should be on containment, minimising the spread, as well as checking whether the infected devices, assets or networks affected the operational running of the vessel, and if so, how quickly can they be brought back to seaworthiness.

In reality, cyber attacks are multi-staged and can take some time to deliver and manifest. In shipboard systems in particular, it is less likely to be a flash-to-bang scenario given the operating environment. So the sooner you are made aware of the initial intrusion, the earlier you can take action.

Investing in the right cybersecurity capabilities can allow you to stretch the response window timeframe. If you were to continuously collect and analyse onboard data before a cyber breach occurs and put this information in the hands of the right people in your organisation, then instead of having hours to respond, you might have days or even weeks. This type of data can help identify key vulnerabilities and the vectors of attack onboard which might be exploited, alongside weak or failing security controls.

Very few of the business leaders considered Phase 4. Yet, how this phase is handled has a significant bearing on loss recovery and minimisation for the fleet owner. Once the incident is contained, assuming the losses are worth the effort, the difficult work of establishing the fact base begins. This typically involves undertaking forensic data analysis to try and understand how the breach occurred in the first place, both to support claims, disputes and regulatory investigations and also to ensure that you don't leave other systems open to the same type of attack. Cyber criminals are notorious for circling back to "double tap" the same victim, particularly one that has established a pattern of paying ransoms.

Digital forensics can be an impossible task if the onboard systems have not been configured to collect and store the right data. Having independent means to collect the onboard data would help solve this problem and puts you in an advantageous position to support deeper analysis of these incidents.

The cyber drill in action

Covering exposures

Number 2, cyber security is not just a technical or compliance problem. Cyber risk management in shipping is primarily a commercial issue and ultimately about ensuring you are protecting against your key financial exposures. The key question business leaders should be asking themselves: Do you already know the extent of your commercial exposures in case of a cyber security incident?

While this might seem a straightforward question, the answer is far from it.

An obvious starting point is the cost of the attack itself. What is the cost of any ransom and restoring operations? This is rapidly followed by determining any exposure to your charterers, due to delays and operational disruptions.

What is less clear is the extent that any of these losses can be recovered, if at all. How clear are you on the extent of your insurance cover, your excesses and limitations, as well as residual risks that are not covered?. Many hull and machinery covers already explicitly exclude cyber risks. One factor of standard P&I cover hinges on whether the cyber-attack is considered to be an attack of terrorism – and that depends upon the motivation behind it. Establishing the motivation for an attack may not necessarily be easy to do, unless there are clear signals like a ransom note. In any case, the policy holder needs to demonstrate that they did not act in an "imprudent, unsafe, unduly hazardous or improper" way.

What about the responsibilities and liabilities of your suppliers? For example, the shipboard system vendors and integrators or visiting service engineers. Who has liability for losses arising from a cyber-attack that originated on their systems and to what extent has that been clarified contractually?

These supplier and insurance agreements are vital to being able to recover and limit your exposures. So, if you don't already have access to a single aggregated view, start now.

Comms control

Number 3, communication flow during a crisis is vital. When a cyber security incident hits, it's likely to be only the IT team that has the knowledge to understand the seriousness of the incident. How can you balance the need for continuous flow of information with the need for laser focus on incident containment in order to support vital management decisions?

While assignment of roles and responsibilities is natural as part of incident response, it can be too easy to overlook the importance of delivering clear and consistent messaging throughout an incident. It isn't simple to express complex, technical issues in layman terms, a skill which is vital in communicating effectively to all stakeholders during a crisis. Investing in training and cyber drill practices can help improve the efficiency of internal communication.

Organisations should not overlook the importance of crisis communication when formulating business continuity plans or when staffing emergency response teams.

Number 4, no two crises are the same. Drills help your team think on their feet. How will I know whether we are ready? Awareness is changing, certainly based on the evidence within the room, and across senior business leaders, otherwise this type of question wouldn't have been posed to the expert panel.

"Cyber criminals are notorious for circling back to "double tap" the same victim, particularly one that has established a pattern of paying ransoms"

The starting point is to have a set of structures and protocols in the business to help you mobilise your internal team and create your readiness-to-respond framework. All too often cyber drills, or table-top exercises follow the same process or pattern. However, when faced with a real incident, you are unlikely to follow your response plan exactly. Throw in the tensions that are usually not accounted for in a drill across the different parties: charterers, owners, technical managers, insurers etc, and the difference between practice drills and reality is amplified even further.

To survive a cyber incident, what you need to do is help your team think on their feet. This is where regular drills are helpful.

In order to prepare effectively, consider changing your internal cyber drill scenarios and prepare your team to respond to new situational challenges. One of the most effective ways to test this is to engage external organisations that have expertise in the type of cyber security scenarios you are likely to face across the entire organisation.

Legal pitfalls

Number 5, avoid compromising your legal privilege. When an incident or investigation first arises, companies can respond in different ways. Some will look towards their in-house legal and/or compliance teams or through an internal investigation team. Others will appoint external advisers to assist with the investigation typically by instructing lawyers to carry out forensic reviews or to conduct the investigation.

It is crucial to carefully consider the sequence of instructing your lawyers. Instruct them early and you can orchestrate it such that all the investigation gets protected under legal privilege. Instruct them late and the evidence surfaced from investigative work may not be privileged. This could come back to really haunt you in a dispute situation.

A final thought: one of the critical elements of cyber risk management is ensuring the appropriate level of executive commitment and engagement within the organisation. Inevitably, senior commitment to cyber risk management will heavily influence the way risk practices and cyber strategy becomes embedded within the business.

The goal for this event was to build increased awareness and understanding of cyber risks across the leadership team. In that respect, the drill helped this group of senior executives think about their possible areas of exposure and effective mitigations.

Ultimately, business leaders want to make intelligent and risk-based choices on a day-to-day basis, underpinned by data and clear insights. The challenge when it comes to cyber security is that this is a topic that requires deep knowledge and expertise in an industry that is only just starting its regulatory and security journey.

Managing the risks and improving cyber resilience begins with knowing which questions to ask internally. Now is the time to start asking those difficult questions, not when a cyber-attack happens. **SN**

Richard Wagner is business development director for the Asia-Pacific region and Daniel Ng is CEO of CyberOwl. The company – founded as a spinout from Coventry University, Crossword Cybersecurity PLC and with funding from Mercia Fund Managers in 2016 – leverages data and analytics to shift organisations towards an 'active cyber posture'. For more information, go to www.cyberowl.io.

The cyber drill team considered the risks of a cyber incident

In-depth defence to protect landside assets

IAPH's Pascal Ollivier explains why ports need to take cyber risks more seriously

Pascal Ollivier

Shipping Network: What is the biggest cyber-related threat to ports today?

Pascal Ollivier: The primary motivation of most cyber threat actors is financial gain when it comes to ports. The latest trend is the increasing use of indiscriminate ransomware attacks propagated via phishing mails. The direct targets may not be ports themselves, but these attacks are sustained and constant and have impacted ports in the past. The Port of Los Angeles, the busiest container port in the US, has seen a 50% increase in unauthorised intrusion attempts since the beginning of the pandemic which have reached 30-40 million per month.

Topic: Ports

Keywords: Information sharing, zero-trust, guidelines

Background: Ports need to develop strategies of protection, detection and mitigation for cyber attacks

SN: Does that threat differ for the multinationals versus the small, single port operator?

PO: As far any port is concerned, the threat remains the same.

SN: I recently heard cyber security described as a journey, not a destination. Do you agree with that statement?

PO: Yes indeed, I would agree with that. It requires a cultural change within organisation. The weakest link can end up being the strongest one, namely the human element.

SN: Can ports ever be confident that they have cyber security 'under control'?

PO: Rather than taking the approach to have cyber security under control, ports should adopt a more defence-in-depth strategy based on a zero-trust framework. This is outlined in the IAPH Cybersecurity Guidelines. Every port will inevitably be on the receiving end of an attack, the question is how the port protects, detects and mitigates.

SN: How is IAPH supporting and encouraging its members to report more to improve knowledge sharing?

PO: Information sharing should be managed at multi-layer levels: port community (port eco system), national (Defence, Homeland Security), international (such as PACC-NET and ChainPort).

SN: How has Covid altered the port cyber risk landscape?

PO: It has exponentially grown due to the acceleration of digitalisation and the new tendency towards remote working.

SN: What was the catalyst for the creation of the IAPH Cybersecurity Guidelines for Ports and Port Facilities?

PO: Back in Q2 2019, IAPH conducted an internal survey at port authority level on cybersecurity. As the port community was found to be a weak spot, IAPH launched the Port Community Cybersecurity awareness paper in 2020. This is turn led to the need to develop more comprehensive cybersecurity guidelines for ports and port facilities in a manner consistent with IMO Maritime Cyber Security guidelines.

SN: What are the next steps for the guidelines?

PO: The IAPH Cybersecurity Guidelines were submitted to the IMO on July 2 and were received very well. They are now passing through the IMO Trade Facilitation Committee with the eventual ambition that they are considered for referencing in the next version of circular MSC-FAL.1/Circ.3/Rev.1 Guidelines on Maritime Cyber Risk Management.

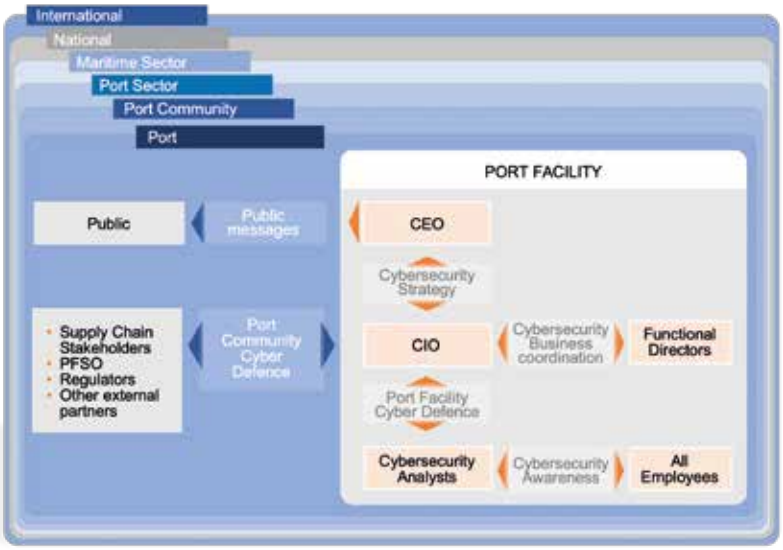
SN: What do ports need in terms of resources to effectively manage cybersecurity risks?

PO: These Guidelines address the concept of how much is enough. Based on creating a profit loss scenario in terms of risk management, the first step a port needs to take is a Business Impact Analysis as ports are in themselves critical infrastructure when it comes to the maritime trade supply chain.

SN: What challenges do ports face in moving from reactive towards proactive cyber resilience?

PO: Right now, priority no.1 is to get the CEOs and their respective executive boards highly engaged and organised to combat this threat. ***SN***

Pascal Ollivier is the International Ports and Harbors Association data collaboration chair, www.iaphworldports.org.



Dashboard of the IAPH Cybersecurity Guidelines

Cyber: a new frontier for seafarers

The Mission to Seafarers' Ben Bailey sees a vital role for crew in safeguarding vessels from online attack

Ben Bailey

As William Shatner blasted off into space, tech-lovers' eyes turned to the machine which propelled him. Two thirds smaller than a fully assembled NASA shuttle, the fifty-nine-metre-tall *New Shepard* propelled four members of the public 66.5 miles to the front door of space. There was no crew on board (the captain of the *USS Enterprise* doesn't count, apparently), and the ship was entirely controlled by on board computers. Even ground monitoring was minimal, though presumably had something failed, someone, somewhere could have taken control and attempted to return it back to earth.

Topic: Seafarers

Keywords: Digital, accessibility, training

Background: Crews can be both the weakest and the strongest link when it comes to protecting ocean assets

Such technological and engineering advancements have sparked a new round of debates about cyber security. What systems are in place? How secure is the connection? How do we prevent assets from being hijacked? How safe is our data?

Of course, in maritime, there have long been conversations around cyber security. With so much technology packed into the modern-day vessel, the threat from cyber-attack is real, and the IMO has adapted the ISM Code to account for such threats. New measures, which require signatories to ensure cyber risks are appropriately identified and controlled within safety management systems, were agreed in 2017 and came into effect in January of this year.

Critics of the measures believe more needs to be done, with some calling for an international Standard to be created to which port states and ship owners can be measured against. Others feel that the ISPS Code should be the relevant instrument to deal with this important issue. Regardless of the rights and wrongs and the appropriate mechanism, this subject is only going to grow in importance as technology advances.

For seafarers, their role in ensuring cyber security is vital, and for some industry thinkers, their role in safeguarding a vessel from online attack is just one reason why ships will never be fully vacant of people on board. In addition to the technology already in place, crews often bring with them lots of gadgets and gizmos. From spare smart phones and laptops to the latest PlayStation. If these are not properly checked for ransomware or malware, the consequences could potentially be devastating. Setting expectations and adequate training is therefore vital to ensure everyone is aware of their responsibilities.

"Understanding the digital limitations and restrictions of a life at sea is vital for organisations like ours if we are to produce suitable services for seafarers and their families"

Creating a safe cyber space for seafarers is a natural extension of the work of welfare agencies

Locked out

Having your assets locked down by a foreign entity is terrifying. Five years' ago, my colleagues and I at The Mission to Seafarers came into work one Monday to find our email system had gone down. Our brief pleasure at not being contactable for a few hours quickly disappeared when we realised all our files had been locked too. Someone, somewhere, had hacked into our servers overnight and blocked off our access. Then, after three days, everything was magically released, and we were able to go about our work. A ransom was never paid (or demanded), and fortunately our most protected data – donors' personal details – was unaffected.

The verdict from our IT providers was that someone was trying their newly created hack; we were simply the guinea pig before the attacker sought a much larger prey. The situation, however, was a timely reminder to all of us about the need to protect that which is important – in this case our data, our donors' data, and the systems we use to provide quayside services in 200 ports across 50 countries.

More widely, the maritime industry is investing millions to protect itself from rogue attacks. Failure to do so could create a safety or environmental disaster, not to mention disrupt the international supply chains on which the world relies. But while

these areas are important, is there a case to safeguard a holistic space in the cybersphere for people to share information, create value, and seek help and advice?

Creating a safe cyber space for seafarers is a natural extension to the Mission's in-port services, particularly in these Covid-19 days when new avenues of service provision have been required. When the very first lockdown was imposed across the UK, many elements of our work shifted online. We developed a Chat to a Chaplain service, which allows seafarers to speak to our teams 24/7. Accessed via our website, seafarers can talk to one of our trained port chaplains or welfare officers and ask us about a wide range of issues.

Eighteen months on, a cursory review of the topics reveals the issues of our time: requests for local information, concerns about catching the virus, accessing the vaccine and fears for loved ones back home. As borders closed and the shore leave crisis deepened, seafarers contacted us with details of alleged abandonments and asked for our help in providing supplies and support.

Our CrewHelp service – where seafarers can find assistance with issues ranging from questions about their contracts to emergency financial aid – regularly receives copies of contracts, seamen's books, and other personal information which, in the wrong hands, could be used for inappropriate means.

Service for seafarers

Understanding the digital limitations and restrictions of a life at sea is vital for organisations like ours if we are to produce suitable services for seafarers and their families. It's one of the reasons we created our WeCare Social Wellbeing programme – an e-learning course which explores the link between online activity and the impact it can have on our mental health. Through animation, quizzes and games, the course provides ways to ensure we and our loved ones can stay safe online and not breach our company's IT policy while safeguarding our personal data. To date, over 15,000 seafarers have been given access to the programme.

Currently, much of my team's work is focused on delivering an app for seafarers to access our services, which we hope will be available in January of 2022. The yet-to-be-named offering will allow seafarers to pre-order services from our teams across the world – from local items of shopping to requesting a ship visit, transportation, as well as a check in function to our seafarers' centres to gain access to our free Wi-Fi.

But as much as the app will be practical, we also want to create a space for seafarers to learn and take charge of their mental health. The Seafarers' Happiness Index will be available for those who wish to track their personal satisfaction levels throughout their contract, as well as access our On Board Mental Health Champions material, which provides tips and tricks for seafarers wishing to boost their mental health while away from their familiar support structures of family and friends.

All of this requires strong, secure networks to ensure not only that the data of our users is protected, but that seafarers feel they are in a safe space where they can talk to us about the same issues as they would were one of my colleagues on board, sitting in the mess having a face-to-face chat.

Before Shatner went into space, he reflected on the technology and data involved to make his ten-minute voyage possible. "I'm going up in a rocket and our best guess is it should be fine," he told an audience at a Comic Con in New York City. "I'm terrified. I'm Captain Kirk and I'm terrified."

While most of us will never get the chance to orbit the world in a state of weightlessness, we can boldly turn our attention to cyber security – a frontier which is much closer to home. **SN**

Ben Bailey is the director of advocacy for The Mission to Seafarers, www.missiontoseafarers.org.

Crews often bring technical gadgets and gizmos onboard with them, increasing cyber vulnerabilities

Decarbonisation – a marathon, not a sprint

Carly Fields hears why shipping needs to reward first movers and take decisive climate change action

Carly Fields

"Go green or go home" – that was the challenge set by Alderman William Russell, the Lord Mayor of the City of London, at London International Shipping Week in October.

Alderman Russell threw down the decarbonisation gauntlet to the shipping and wider trade industries, stating that trade does not need to stop to achieve environmental goals.

His view was shared by Soren Toft, CEO of Mediterranean Shipping Company: "Meeting global trade demand must not be decoupled from the urgent need to meet decarbonisation ambitions. We must develop new technologies at a pace we have never seen."

Dr Tristan Smith of the UCL Energy Institute at the University College London said that the industry cannot afford to rest on its laurels, even with a global pandemic disrupting life and trade. "We don't have two years where we can put everything on hold," he said. Therefore, the policy process needs to keep moving.

But the bottleneck that needs to be addressed is new fuels at scale. Dr Smith said ships have four basic options: batteries, nuclear, biofuels, and hydrogen-derived biofuels. Through a process of elimination – "you can't put batteries on deep sea ships, or nuclear, and biofuels have constraints on sustainable supply" – hydrogen is the pathway the industry has to consider. "It's probably not hydrogen itself," he said, "it's a liquid renewable energy. It's a means of us having a closed loop on energy, which enables sustainability."

Dr Tristan Smith said that hydrogen is the pathway the industry has to consider

'Decisive decade'

In light of the challenge facing the industry, the 2020s must be the "decisive decade", said Nigel Topping, the UK's high-level climate action champion for COP26. "It's time for shipping to turn ambition into action and join the Race to Zero." The Race to Zero is a global campaign to rally leadership and support from businesses, cities, regions, investors for a healthy, resilient, zero carbon recovery that prevents future threats, creates decent jobs, and unlocks inclusive, sustainable growth.

Mr Topping said it will be too late if shipping waits for complete clarity on the fuel of the future before advancing. "The risks are too great if companies fail to understand the inevitability of this

Liner normalisation 'within 12 months'

The leader of one of the world's largest container lines said he expects to see a normalisation of surging global container trade within the next 12 months.

Soren Toft, CEO of Mediterranean Shipping Company, described the environment for global trade as "unstoppable" at the moment, warring between "raging demand for trade and physical goods" and "tangled supply chains".

The peak trade being experienced now is the result of shipping 12 months of goods in eight months – which is where the problems started, Mr Toft said. During the first seven months of 2021, MSC saw a 33% increase of imports from Asia into the UK.

"While the supply chains are vast, they are not built for those kinds of increases," he said. "There was no buffer capacity when things went off the rails."

Once trade normalises, Toft expects to see a cool down and he will be happy to see some pressure taken off liner shipping

MSC's Soren Toft spoke of 'raging demand' for trade

teams. "From morning to night, our people are dealing with problems. We are trying to solve them, dealing with stress and long work hours." *SN*

The LISW panel discussed decarbonisation challenges and opportunities

direction. Ship owners, charterers, fuel producers, investors and other actors with an ambition to thrive in the coming decade must turn rhetoric into formal commitment and then start delivering on short term plans," he said.

First mover projects were applauded by the panel for propelling research and development into and understanding of the decarbonisation challenge. Katharine Palmer, shipping lead of the climate champions, said that first mover projects give the industry the learning that is needed to scale future deployment. "It will be an opportunity to reduce costs," she said.

While the panel agreed that there are opportunities being a first mover in shipping, there are also concerns. Claes Berglund, director public affairs and sustainability at Stena AB, said that Stena converted one of its ships to methanol in 2015 at a total cost of €22m, part funded by the EU Commission. "Were we an early mover or a Betamax? We still don't know," he said. "You need to have a long-term perspective to de-risk a vessel."

Lyras Maritime's CEO Markos Lyras suggested better incentivisation of early movers. "We can only learn from experience," he said, noting that some early movers looking to meet the Ballast Water Convention requirements were penalised.

Design development

Lloyd's Register CEO Nick Brown said he is confident that designs for deepsea zero emission vessels will be available within two years. "The technology hasn't been waiting for further guidance," he said. "We think that the real focus for the next two years is to get demonstrators and pilot projects going to learn from and get projects to scale." The focus needs to be squarely on 2030, he added, and momentum needs to get going now.

Tim Wilkins, environment director at Intertanko, took the impetus a stage further: "If we miss 2030, 2050 becomes a pipedream. The next two years will be critical for the shipping industry. The decisions taken in design, construction and propulsion of these vessels will need to be made now."

Ms Palmer noted that there is the question of funding large scale demonstration projects and the challenge of making the sector investable. The biggest shift, however, is with global mentality, said Mr Lyras. "We are all working together to find a solution that would normally take 10 years in one year. Start with the problem we are trying to solve and get to a solution. Shipping is a business, so we have to make it possible," he said.

The pros and cons of carbon pricing and regional regulations were also debated by the panel. Aoife O'Leary, the director of international shipping and carbon pricing at the Environmental Defense Fund, said she found it interesting that the industry and those affected by climate change are debating carbon pricing. "It's not that hard: you put a price on pollution and then use that money to address that," she said. "We have all the tools, we know what policy we need – what are we waiting for? Let's just get it done."

Dr Smith added that there is nothing to fear from regional solutions and national actions. "We need to have that going on. This idea that there is a challenge to the authority of the IMO by having EU regulation and national government taking proactive action is false and misplaced. When we do have the IMO solution – which I'm convinced we need – we need to reduce the costs. If we come to the IMO with solutions in place, we will move much faster."

However, MSC's Mr Toft was less accepting of regional regulation. "Regionalisation will lead to retaliation which will lead to complexity and a more expensive supply chain," he countered. "Shipping is what connects us all. We think that it should be real global solutions and regulation."

The Rt Hon Anne-Marie Trevelyan MP, UK international champion on adaptation and resilience for the COP26 Presidency and Minister of State for business, energy and clean growth, neatly summed up the challenge facing the industry: "This journey to decarbonisation is a marathon, not a sprint – but that doesn't mean you can stop for a coffee on the way." ***SN***

"Ship owners, charterers, fuel producers, investors and other actors with an ambition to thrive in the coming decade must turn rhetoric into formal commitment and then start delivering on short term plans"

Increasing complexity of the marine space

NLAI's Phil Buckley urges a more cohesive rethink of the use of our seas and oceans

Phil Buckley

Coastal and offshore regions are supporting increasing levels of human activity and the next 20 years are likely to see a massive increase in economic activity.

The maritime operating environment already comprises a complex mix of law, practice, custom, agreement and commerce. Seafarers understand that the sea is a vast, often tumultuous highway along which the traded goods of the world flow; everyone else possibly sees a near-infinite, empty, unused expanse, ripe for development. In coastal areas the expansion of urban growth and economic exploitation into the sea will add further to the physical and legal complexity of the marine space.

Offshore wind, for example, is set to play a massive role in bringing the UK towards carbon neutrality by 2050, significantly reducing the navigable sea-space in the waters around the British Isles. This is further impacted by the ever-advancing pace of technological innovation in the renewables sector. As the Financial Times reported at the start of August, investment in offshore floating wind is accelerating significantly. These floating structures can be deployed much further offshore – in depths over 70 metres – where winds are more powerful, and they are not as prominent visually. Equinor's Hywind Scotland floating wind project, for example, is approximately 25 kilometres (circa 15 miles) off the coast of Peterhead. This is great news both for capacity and for local communities who want offshore renewable structures to be out of sight and out of mind; however, they create another potential navigation issue for mariners and such offshore locations are often very hostile environments for all users.

The same is true (or may soon be) for offshore aquaculture. Several reports – including The Value of Scottish Aquaculture by the Highlands and Island Enterprise and Marine Scotland – have noted that moving fish farms further out to sea may be necessary to meet ambitious growth targets and address environmental concerns.

Then, of course, we are entering the age of autonomy at sea, with Saildrone's recent Pacific crossing just the latest in many milestones pointing to a more congested, and uncrewed, maritime space.

Thus, a massive increase in economic activity in the next 20 years will involve a substantial proliferation of artificial structures, energy farms, power generators and aquaculture while our current fixed marine infrastructure and port facilities are also likely to increase in complexity and footprint.

Just as we really ramp up our use of the sea it, in turn, will challenge our heavily populated and developed coastal and offshore regions through the consequences of climate change with rising sea levels, extreme weather effects and other natural events.

Overcoming challenges

Shipping (and by inference the wider Blue Economy) faces a range of challenges that include changes to shipping trades and patterns; new technologies and innovation; the regulatory framework and shipping decarbonisation; and digitalisation. The pace of change will have to increase to meet declared targets and will demand the implementation of new policies that will depend on and generate a significant growth in e-navigation and other marine environment data services. A proper understanding is needed of how increased use of the sea space, changes and growth in shipping and changes to patterns of marine traffic density and routes will all impact safety at sea.

Implementation of new policies will depend on and generate tremendous growth in marine data including, but not limited to, e-navigation. The International Maritime Organization (IMO) defines e-navigation as "the harmonised collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means to enhance berth to berth navigation and related services for safety and security at sea and protection of the marine environment".

Beyond the definition, there is also an IMO Strategy Implementation Plan that recognises that this is a fast-moving sector due to technology changes, so demands constant review and reflection.

Is it time for the UK Marine community to work out how e-navigation could be delivered around the British Isles in order to support the UK's legal obligations, recognising that the congested seas around the British Isles are only going to become more complicated? Should we be trialling potential Sea Traffic Management (STM) services in projects such as Accessibility for Shipping, Efficiency Advantages and Sustainability (ACCSEAS) to ensure the safe, effective and sustainable management of UK waters?

The challenges of sharing sea space have become more pressing

e-Navigation and STM

The need for comprehensive water space management in this busy corner of Northwest Europe is obvious and unavoidable. Shipping routes that are heavily constrained by offshore infrastructure will need positive control from major vessel traffic control centres and such centres will utilise continuous real-time tracking of all blue economy activity at sea through a comprehensive common operational picture including SOLAS, recreational and all types of shipping.

Increasing complexity of our seas is likely to require increased surveillance and the fusion of multiple sources of data to improve safety and security through improved situational awareness in Territorial Waters (and ideally the entirety of the EEZ). Situational awareness would include trends and changes in traffic patterns and navigational risk assessment; real-time applications for route optimisation; and deconfliction ahead of potential collision situations.

STM as a concept is at a mature stage of development in on-going validation projects in Nordic and Mediterranean seas. e-navigation offers a myriad of data types to users in service of ship-based navigation although the current overlapping and multi-faceted product landscape, with differing stages of maturity and utility, is causing confusion and uncertainty. There is a very wide range of data 'available' in coastal regions and the challenge is to understand what is (or might be) useful – and what is (or is not) e-navigation.

The relationship between STM and e-navigation is not yet clear. The UK could develop its understanding, and a strategy, through imaginative use of a Digital Twin to identify the utility and applicability of some of the more commonly recognised systems. Using a Digital Twin (a virtual representation of a physical object or process) would result in safer, less environmentally impactful and more time-efficient operations both at sea and in ports, help manage a quickening pace of change and introduction, and avoid the potential for a lack of coherence and coordination. This could lead to the development of STM solutions in particularly challenging areas and maybe as extensions to the controlled waters off some of the UK's major ports.

Position, Navigation and Timing (PNT) is the backbone of datasets enabling a range of potential future e-navigation maritime solutions and wider added-value services for Blue Economy applications. Resilience and integrity are key with government, industry, and academic organisations interested in exploring terrestrial solutions to improve resilience and integrity. There is a potential role for the General Lighthouse Authorities here if only to use their extensive aids to navigation infrastructure.

Autonomous shipping relies on elements of e-navigation services, especially GNSS, AIS and GPS data. Reliability, accuracy and consistency or 'trust' in PNT data is core to all development and end users.

Connectivity opportunity

The introduction of new services and infrastructure in line with user requirements and technological developments may have regional variation but will be within the overall IMO regulatory framework. A UK/Irish framework within Maritime Connectivity is a clear opportunity with the potential for a regional offering of services within a 'Maritime Service Portfolio'. This will require engagement between service providers, regulators, and innovative industry expertise.

The Maritime Connectivity Platform (MCP) has a clear role here although its governance is not yet fully defined. MCP should be able to help with the evolution towards a 'service culture' which e-navigation encapsulates.

The aim would be the creation of a 21st century reliable, efficient and cost-effective common operational picture for the benefit and safety of all mariners – that is to say, all those who work at sea in all sectors of the blue economy, supported by their counterparts ashore. **SN**

Captain Phil Buckley is a retired Royal Navy submarine commanding officer and former harbour master at Jersey and Southampton. He is an associate at NLA International assisting with Blue Economy solutions for a range of maritime authorities.

The nightmare before Christmas

S&P Global Platts' Wyatt Wong makes sense of organised chaos in the LNG shipping markets

The liquefied natural gas (LNG) shipping market is typically highly cyclical, with fortunes made and lost through the strong northern hemisphere winter months of November through to February. Winter 2020-21 was among the most extreme markets in recent memory, with record time charter rates for LNG carriers accompanying record commodity benchmark prices. Given the record levels achieved last winter, what could be in store this coming Christmas season?

In this article we will look at some of the factors that caused such chaos in the market last winter, what has happened since then, and the forces shaping the market for winter 2021-22.

Last Christmas

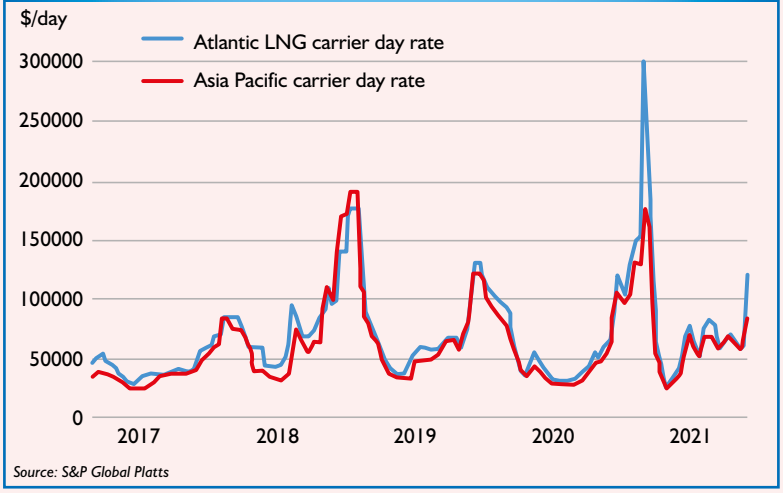
On January 8, 2021, BP was reported to have paid the equivalent of $350,000 per day to fix the 170,000 cubic metre capacity LNG Abalamabie for a transatlantic voyage – the highest recorded rate paid for a cargo ship in history. However, it's easy to forget that before such headlines, LNG shipping rates had been wallowing near three-year lows for much of 2020, until the final quarter. The first-to-third-quarter in 2020 averaged $43,151 per day, only higher than the lows last seen in 2017 at $36,211 per day. The low shipping rates mirrored the LNG cargo market, where the S&P Global Platts Japan Korea Marker (JKM), the North Asian benchmark price for LNG, was in the low-$3s/MMBtu level, also a three-year low.

The low-price LNG environment was due to weak demand, with high stock levels across both the Atlantic and the Pacific. US LNG cargoes – a source of demand for LNG shipowners – were also cancelled throughout the second and third quarter of 2020, which partly explains the bearishness in LNG spot shipping. In May, twelve cargoes were cancelled, while from June to August between 35 to 45 cargos were reported as cancelled each month. Twenty-six cargoes were cancelled for September and nine cargoes for October loadings. These cargoes were not lifted as they could not price profitably into Europe and North Asia.

Slight increases in LNG shipping rates began in mid-August 2020: from mid to high-$30,000s per day on August 14 to high-$40,000s per day by early September. However, this optimism was short-lived, as rates fell on the back of uncertainty due to production problems at the Cameron facility in the US Gulf due to Hurricane Laura which hit the region late August. "Sentiment was bullish running into September but an unfortunate hurricane in the US Gulf has turned it around," said a shipowner source at the time.

Owners' bearishness was mirrored by the other side of the market too: "If things don't change we won't get to six figures as there is no bullish news, but things can change quickly given thin supply in the Atlantic," said a charterer source to Platts in September.

LNG Shipping Rates



Source: S&P Global Platts

Against all odds

Yet, against expectations, the LNG shipping market turned shockingly bullish over Q4 2020. The Atlantic shipping rate increased from $105,000 per day to an all-time high of $300,000 per day between November 30 and January 8 – an increase of 185%. The Pacific LNG shipping market also rose from $100,000 per day to $175,000 per day during the same period, rising 75%.

LNG shipping rates averaged at $93,239 per day over Q4 2020 and Q1 2021. This is in line with the average over the winter of 2018 at $100,713 per day, and is stronger than the $63,647 per day, $81,564 over the winters of 2017 and 2019 respectively.

The strong gains in LNG shipping mirrored that of LNG. The JKM increased from $5.163/MMBtu to $32.500/MMBtu, from October 1 to January 14, gaining 529%. The JKM averaged at $8.882/MMBtu over the winter of 2020, surpassing the averages of the previous two winters, at $4.687/MMBtu and $8.294/MMBtu respectively. The gains in JKM were attributed to robust prompt demand from North Asia, as cold temperatures swept the region – China, in particular, has seen year-on-year LNG import growth since April 2020.

The winter of 2020 was a turning point for LNG and LNG shipping as they emerged from three-year lows. High LNG prices resulted in a wide arbitrage window to send Atlantic cargoes into the Far East, creating demand for

spot voyages and higher ton-mile. Meanwhile on the supply side, there was a consensus in the market that shipping was extremely tight for February spot loads in the Atlantic. "There are no ships in February in the west," said a charterer.

As the LNG spot shipping market continued to boil, more aggressive action was reported. Trafigura was heard to have issued a firm bid for H1 February US Gulf load, to deliver into Europe, at $350,000 per day with a ballast bonus of $4.75 million. This bid was then followed by BP's record-breaking fixture of the LNG Abalamabie at $350,000 per day round-trip basis for January 20 to January 25 Freeport load, delivering into Europe.

The combination of low vessel supply in the Atlantic and a wide arbitrage window to place Atlantic cargoes into North Asia had created an environment for this record-breaking fixture, a historic high.

Back to normal?

The LNG shipping market returned to its cyclical ways by late March 2021, sinking to the low-$30,000s per day level. Between early April 2021 to mid-May 2021, LNG shipping rates rose from $33,750 per day to $68,500, due to the combination of low vessel availability and an open arbitrage window to place Atlantic cargoes into North Asia. JKM increased from $7.088/MMBtu to $10.394/MMBtu, from April 1 to May 17, gaining 44%. In shipping terms, the summer of 2021 averaged at $59,087 per day, which was higher than the averages over the past two summers at $35,904 per day and $53,857 per day respectively, but in line with the summer of 2018's $61,885 per day.

A recurrent theme since the price hike last winter has been high activity in the multi-month charter market. Platts heard 43 fixtures, with the charters covering at least up to the start of the coming winter and are up to two years long. Of those fixtures, 35 of the ships have a capacity of 155,000 cu m or above, indicating a preference for bigger vessels that are more economical in a high-price LNG environment. Nineteen different charterers were rumoured, including majors such as Total and traders such as Trafigura and Vitol.

The way forward

So, what can we expect this year? Spot tonnage availability is low across both the Atlantic and the Pacific. Part of this reason is structural, as independent owners have all but disappeared from the spot marker due to the flurry of multi-month charters described above. "All vessels from independent owners were gone, you only saw relets in the market," a shipbroker said. A shipowner source agreed: "Vessels were in control from traders, the spot market for shipowners simply did not exist," he said.

The strength of European gas and LNG prices also mean that vessels are likely kept for own use as opposed to being offered into the spot market.

TTF – Title Transfer Facility, the Northern European gas benchmark – increased from $6.569/MMBtu to $32.83/MMBtu between April 1 and October 7, increasing 400%. Low storage levels, caused in part by lower flows from Russia to Europe, were the key fundamental drivers. Meanwhile, JKM had also increased from $7.088/MMBtu to $35.604/MMBtu over the same period, increasing 402%, and also touched a new high of $56.326/MMBtu on October 6. Persistent short-covering demand from trading houses and portfolio players in the Far East and a historical rally in the TTF market kept Asian spot LNG prices buoyed.

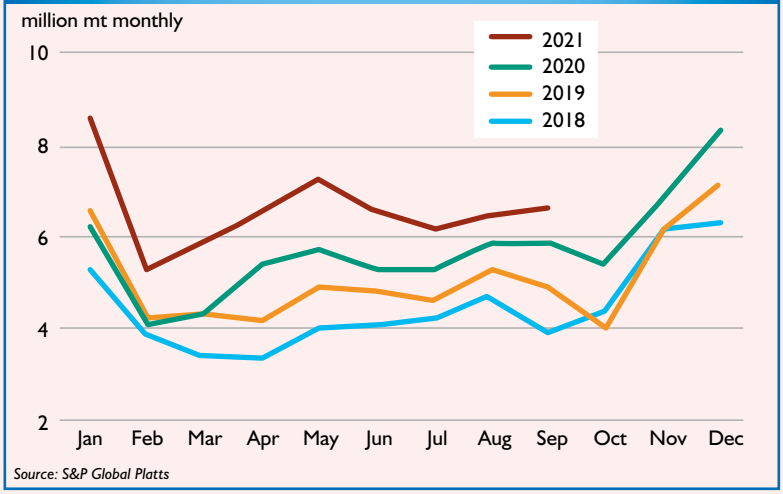
If the JKM vs TTF spread remains narrow there will not be a reposition of vessels from West to East, and so ton-mile will stay low. But how much LNG shipping prices can continue to rise remains an open question. Market participants' opinions are mixed on what lies ahead for LNG shipping in this year's last quarter, although all agree that higher rates are to be seen starting November. Some, though, expressed concern and estimated that higher LNG prices could have an unexpected effect on shipping.

"Luckily we did our Christmas shopping back in May," said one charterer source to Platts in mid-October. "We're hearing $200,000 per day levels in the Pacific for December already, and I wouldn't want to be caught short now." SN

Wyatt Wong is the editor for LNG Shipping at S&P Global Platts. For more insights, please visit www.spglobal.com/shipping.

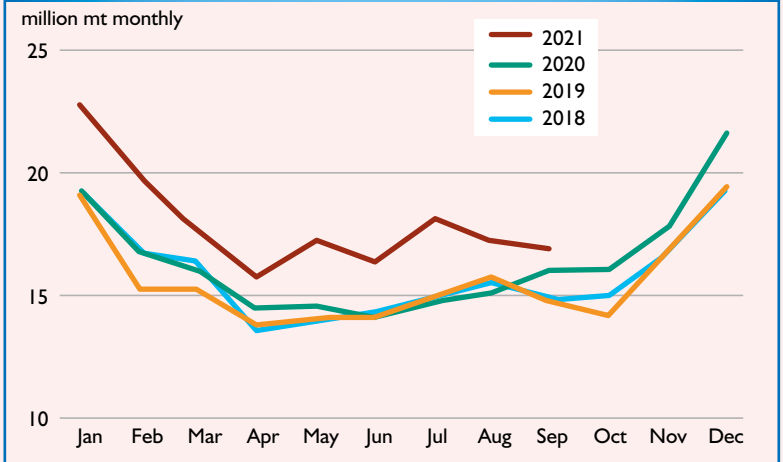
S&P Global Platts

China LNG Imports



Source: S&P Global Platts

JKTC LNG Imports



Source: S&P Global Platts

Homage to Paper

Weird and wonderful facts about one of the shipping industry's commodities. This month, we take a closer look at paper.

Paper is almost **2000** years old.

It was invented by the Chinese around **105 AD** and was kept a secret for many years

Our English word "paper" is derived from the word **"papyrus"** in Egyptian

A pine tree can produce about **80,500** sheets of paper

The first book that was printed from industrially made paper was produced in **1804** – John Anastasius Freylinghausen's *An Abstract of the Whole Doctrine of the Christian Religion*

In 2019, the global paper and pulp market size was valued at **$348.43 billion** and is expected to reach the value of almost **$370 billion** by 2027

The average office worker handles around **10,000 sheets of paper** every year

The **US** and **Germany** are the leading paper importing countries, accounting for about **10%** and **8%** respectively. American businesses use enough paper every day to **circle the globe 20 times**

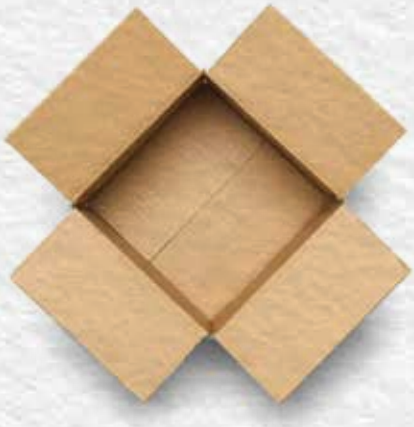
The largest paper consuming country worldwide is **China**, with over **100 million metric tons** of paper and paperboard consumed each year

Paper and cardboard have one the highest recycling rates of any waste material.

Globally, the use of paper and paperboard generates more than **100 million tons** of paper waste every year.

70% less energy is needed to recycle paper and reuse it compared with making it from raw materials.

Every tonne of paper that gets recycled saves **7,000 gallons of water** and produces **73%** less air pollution than producing paper from new materials. Recycling one ton of paper saves **17 trees**



The most in-demand type of paper worldwide is **containerboard**, which is used to make corrugated boxes (or cardboard) and is typically used for packaging solutions

Not all paper is made from wood; it can also be made from **scraps of cloth and pieces of hemp material**

Sources: www.statista.com
www.papermilldirect.co.uk/inspire/10-interesting-paper-facts
www.jampaper.com/blog/interesting-facts-about-paper/
www.ryman.co.uk/blog/10-amazing-facts-about-paper
www.historyofpaper.net/paper-facts/facts-about-paper/
Guo, C. Utilization of Waste Paper in China and Market Situation of the World in 2018 (In Chinese); 2018. [Google Scholar]

Legal Eagles...

Do you have a burning legal question for the HFW *Shipping Network* team? Email legaleagles@ics.org.uk for them to answer your question in the next issue of *Shipping Network*. Questions should be of a general nature and not specific to a particular live issue.

HFW's crack team of specialist shipping lawyers answer your legal questions

Henry Clack

Guy Main

Anthony Woolwich

Q What are the consequences under the EU and UK GDPR of a cyber-attack resulting in a personal data breach?

A First, what is a personal data breach? The EU GDPR and UK GDPR define a personal data breach in Article 4(2) as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data…". This can be any event which results in personal data being compromised, not just the loss or theft of this data.

Second, if a breach occurs, who needs to be notified and when? The EU GDPR and UK GDPR provide that as soon as the controller becomes aware that a personal data breach has occurred, it should notify the relevant supervisory authority without undue delay and where feasible not later than within 72 hours after becoming aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. The types of risk covered may include discrimination, identity theft, fraud, financial loss, damage to reputation or confidentiality, emotional distress and physical and material damage. Should notification be given after 72 hours, the controller must explain why the delay occurred. In the UK the relevant authority to be notified is the Information Commissioner's Office.

Under Article 34 of the EU GDPR and UK GDPR, when the personal data breach is likely to result in a high risk to the rights and freedoms of an individual, the controller should communicate the personal data breach to the individual without undue delay.

Large fines

Under the UK GDPR, failure to notify a breach can result in a fine of up to £8.7 million or 2% of a company's global turnover, whichever is higher. There are equivalent penalties under the EU GDPR.

If the personal data breach is suffered by a processor, it must inform the controller promptly so that the controller can comply with its obligations (as set out, above). The processor is not required to make any further notifications.

Third, what information needs to be provided when giving notice of a breach? Article 33 of the EU GDPR and UK GDPR outlines the content of any notification of breach to the supervisory authority. This should include at least the nature of the personal data breach, the categories and an approximate estimate of the number of individuals affected. The name and contact details of the data protection officer must be given.

There are clear guidelines for the reporting of a data breach

The likely consequences of the breach should be described, in addition to any measures that have been taken to address and mitigate the possible adverse effects of the breach.

Where the breach requires notification to be given to individuals, the notification should explain in clear and plain language the nature of the breach, the name and contact details of the data protection officer, the likely consequences of the breach and any measures being taken to address the breach and mitigate the impact of the breach. If communicating with individuals would involve disproportionate effort, a public communication is permitted under the EU GDPR and UK GDPR. This public communication must allow all data subjects to be informed in an equal and effective manner. Clear and specific advice on steps that an individual can take to protect themselves should also be given, such as advice on password revisions.

Lastly, when would notification to individuals of a personal data breach not be required? There is no need to notify an individual whose details have been compromised where the controller has implemented protective measures, for example encryption, that render the data unintelligible to outside parties. In addition, there is no need to notify an individual where measures have been taken by the controller to mitigate the risk to the individual to such an extent that there is no longer a high risk to the rights and freedoms of the individual.

Whether or not the breach is notifiable, controllers must document in a breach register the facts surrounding a personal data breach, its effect and any remedial measures taken.

While every care has been taken to ensure the accuracy of this information at the time of publication, the information is intended as guidance only. It should not be considered as legal advice.

Could a failure to implement adequate cyber security protections make a ship unseaworthy?

Many shipowners consider cyber security to simply be a business interruption risk. There is, however, a growing awareness of the issues faced by vessels themselves.

Seaworthiness is relevant to a number of aspects of maritime law and marine insurance. Shipowners are required, among other things, to provide a charterer with a seaworthy vessel, which includes ensuring that it is suitably manned and equipped. The test for seaworthiness is an objective one and involves determining whether a prudent shipowner would consider the vessel fit for purpose, in the relevant circumstances.

Vessels have been found to be unseaworthy for numerous reasons, including defective engines and navigational equipment, and comparisons may be drawn between these examples and those which may result from cyber-attacks. For instance, engine or scrubber management systems may fail due to malware, or navigational errors may arise due to GPS spoofing. Further, given that a vessel's seaworthiness extends to ensuring that it is suitably manned, adequate cyber security training is increasingly important. A lack of training may result in the introduction of malicious software, and mismanagement of a crisis may exacerbate losses. According to Philip Ponsford, deputy chief cyber officer of maritime cyber risk insurer Astaara: "95% of cyber incidents are on account of people." In addition to seaworthiness, cargoworthiness (i.e. suitability to receive the intended cargo) may also be disrupted by cyber-attacks. For example, interference with a container vessel's power management system may result in the failure of the vessel's reefer plugs, causing goods to spoil.

Whether or not a vessel is considered seaworthy has changed over time. Cyber security is becoming increasingly relevant to the industry given the escalating deployment of operational technology on ships, and awareness of the issue is growing, particularly following a spate of high-profile cyber-attacks.

Rules and regulations

The IMO has adopted resolution MSC.428(98) to "raise awareness on cyber risk threats and vulnerabilities". From January 1, 2021, this resolution requires all shipowners to have safety management systems that take into account "cyber risks", and all flag states are required "to ensure that cyber risks are appropriately addressed" by shipowners. The latter point means that vessels risk being detained if cyber risks are not addressed.

While there is greater industry guidance surrounding cyber security (BIMCO, for instance, publish *The Guidelines on Cyber Security Onboard Ships*), there is a lack of clarity as to when a vessel will be deemed unseaworthy due to inadequate cyber security protections. This is because MSC.428(98) and the guidance surrounding cyber security is not prescriptive, which makes it difficult to determine exactly what steps a shipowner should take to protect their vessel against cyber-attacks. Depending on the circumstances of any loss due to a cyber-attack, it might be difficult for a charterer or cargo receiver to successfully argue that a vessel was unseaworthy if a shipowner had taken appropriate steps in relation to cyber security, such as conducting risk assessments and ensuring that crew are properly trained.

The relationship between seaworthiness and cyber is complicated

HFW has this year entered into partnership with maritime cyber security company CyberOwl to assist clients in assessing, monitoring and managing their cyber risks by way of an integrated and commercially focussed service, which extends beyond compliance.

In conclusion, the point at which a vessel will be considered unseaworthy due to inadequate cyber security protections remains unclear. What is certain is that the issue is real, and inadequate security protections could potentially render a vessel unseaworthy, which could give rise to claims from charterers and cargo shippers/receivers. Additionally, if shipowners fail to ensure that cyber risks are adequately addressed, then their vessels risk being detained following port state control inspections. ***SN***

While every care has been taken to ensure the accuracy of this information at the time of publication, the information is intended as guidance only. It should not be considered as legal advice. The articles were written by Anthony Woolwich, Henry Clack and Guy Main. Anthony is a partner, Henry an associate and Guy a senior manager (partner equivalent) at HFW, a sector focused law firm specialising in shipping, aviation, commodities, construction, energy and insurance. Guy is also a Fellow of the Institute and, before joining HFW, he spent 18 years as a shipbroker. Research was carried out by Conor McIntosh and Liam Emmett.

Institute of Chartered Shipbrokers

Follow, like and share your Institute

Find the Institute on your favourite social networks

Search for 'Institute of Chartered Shipbrokers' on LinkedIn, Facebook, Instagram or YouTube to keep up to date with news and developments from the Institute.

Scan the QR codes below to keep the conversation going with your Institute network

LinkedIn main site:

LinkedIn members' group:

Facebook:

Instagram:

YouTube:

Pointing the finger of blame

ITIC's Mark Brattman discusses how and why agents should protect themselves from liability

Mark Brattman

An important protection for any agent is the Himalaya clause found in many bills of lading.

The clause originates from a decision of the English House of Lords in the case of *The Himalaya (1954)*. In that case, a passenger sued the master in connection with an injury sustained while on board the ship.

The passenger ticket contained a clause which protected the carrier from any such action. However, the House of Lords decided that, although the carrier had protected themselves such protection did not extend to the ship's servants or agents who were liable in tort.

Following this decision, ocean carriers included a Himalaya clause in their bills of lading to make sure the defences and exclusions available to the carrier were also available to their servants and agents. The clause applied if (a) it was included in the bill of lading and (b) the act giving rise to the loss occurred during the contract of carriage the bill applied to.

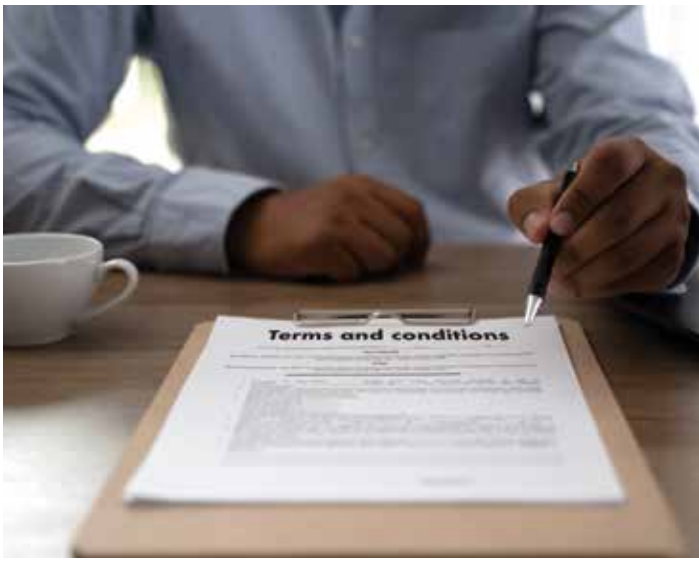
These requirements are seen in *Raymond Burke Motors Limited v. The Mersey Docks and Harbour Co. (1986)*. A container of motorcycles was stored in a container park away from the quayside awaiting the arrival of the carrying vessel when a truck operated by an employee of the Mersey Docks & Harbour Co. struck and damaged it.

The question which the court had to decide was whether the dock company could rely on the Himalaya clause in a bill of lading which had not been issued at the time of the damage. What was relevant was not whether a bill of lading had been issued, but whether the contract of carriage had already come into existence at the time the container was damaged. The court decided that the contract of carriage had not yet come into existence and therefore the defendants were not entitled to take advantage of the clause.

Exclusions

It is worth noting that the clause does not protect (a) the carrier from claims by its customer or (b) the agent from any recovery action by his principal in respect of those claims.

If an agent has the protection of the carrier's bill of lading, why then should they also try and have their own standard trading conditions? One answer is that there will always be circumstances where the carrier's bill of lading terms do not apply – the example above is one such case. Also, in situations where the agent provides services directly to the cargo owner or a freight forwarder, such as arranging the collection or delivery of cargo to the merchant's premises or other final destination or arranging customs clearance services. When undertaking these duties the agent no longer represents the carrier and the carrier's bill of lading terms will no longer apply. The second answer is that the agent can still receive a claim from their principal so they may want to limit liability in those claims.



Terms and conditions do not stand on their own

Having terms and conditions is one thing but they must be incorporated into the contract for the provision of agency services if they are to apply. ITIC has provided advice on how to make sure terms and conditions are incorporated and available on the website here: https://www.itic-insure.com/knowledge/guidelines-on-incorporating-standard-terms-and-conditions-129819/.

In summary, terms and conditions should be brought to the attention of the agent's counterparty before the contract is finalised. Having them signed is the best way to prove that they have been agreed. However, they do not always need to be signed. As long as they have been made available (i.e., referred to in the text of an email or in a header or footer with a link to a copy of them) it could be sufficient to argue they were incorporated into the agency contract. Only referring to them on, say, an invoice would be too late to argue they are incorporated because by this stage, the contract will have already existed for some time. **SN**

Mark Brattman is claims director and legal advisor at ITIC , www.itic-insure.com.

"Having terms and conditions is one thing but they must be incorporated into the contract for the provision of agency services if they are to apply"

Online Academy opens up Institute learning

Digital solutions help students to study at a time and place that suits them

For the last three years, the London School of Shipping has offered a broad range of study programmes to prepare students for the Institute's examinations, leading to recognised shipping industry qualifications.

Classes have been held at the Institute's Head Office in London as well as online.

Candidates who have opted for study through the London School of Shipping have performed well in their exams, demonstrating the great value delivered by the London School of Shipping.

From this year, the Institute will offer the London School of Shipping's traditional classes through its new learning platform: the ICS Online Academy.

The Academy was firstly launched – in its trial version – in April last year to support students disrupted by the pandemic. It was available free of charge until July, when most of the delayed exams were able to be held.

For this academic year, the traditional London School of Shipping evening classes will restart in January, with a new and enriched format via the ICS Online Academy. This study option is designed to help students prepare for their exams in May.

Courses are taught online by Institute recognised tutors, many of whom previously taught in the London School of Shipping faculty. Each subject will be taught with a live session scheduled every second week from January to May.

What to study

Students will be able to enrol for all Professional Qualifying Examination (PQE) subjects via the Academy, in addition to the Institute's Diplomas.

The PQE form the pinnacle of the Institute's qualification leading to membership. They comprise seven exams which can be taken over a maximum of five years. Exemptions may be available to candidates with prior qualifications.

The Advanced Diploma has been designed as a stepping-stone into full professional qualification and suits those who have some industry knowledge. It involves taking two exams: the Institute's benchmark paper Shipping Business plus one other subject from the list of optional papers from the Institute's syllabus.

The Foundation Diploma is ideal for people with little industry experience that would like to gain practical knowledge and a sound qualification. It involves taking two exams: Introduction to Shipping plus one other optional paper.

The Online courses are bundled to include many elements and everything that is needed, from fees, to learning materials, to the assistance of a tutor and more. This includes e-books, live classes, revision, Q&As, forums, masterclasses and workshops, exam prep, workbooks, self-assessment, mock exams, examinations and professional certification.

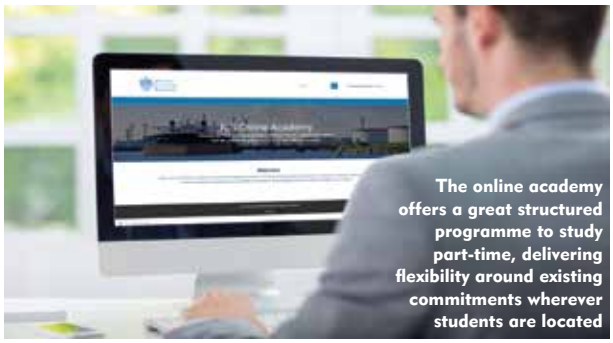
This method offers a great structured programme to study part-time, delivering flexibility around existing commitments wherever students are located.

The fees per online course are £995.00 for the first subject and £895.50 for additional subjects.

Rob Gardner FICS, chair of the Education and Training Committee, commented that the Committee are excited to see the launch of the Online Academy. "The academy is a culmination of hard work put in by the team at Head Office in conjunction with our examination teams and our tutors. It combines the hands-on teaching of our very successful London School of Shipping and our Tutorship distance learning program. This is the first year of its inception and we see it growing to become a powerful tool for you, our students.

"The advantage of it being an online programme is that it is interactive and will build on the input of both our tutors and our students. We believe this will offer students, around the globe, with the opportunity to have the very best of the Institute's tutors just a click away." **SN**

For more information and to book, contact the Institute at +44 (0)20 7357 9722 or shipping-school@ics.org.uk. The form to register for online courses starting at the end of 2021 is available here: https://www.ics.org.uk/ics-online-academy.



The online academy offers a great structured programme to study part-time, delivering flexibility around existing commitments wherever students are located

London School of Shipping – 2020/21 Results

- **83%** pass rate overall (compared to 63% global average across all Institute courses)
- **17%** of passes achieved a distinction
- **100%** pass rate in 6 out of 10 subjects
- **67%** of *Economics of Sea Transport* and *International Trade* students achieved a distinction
- **60%** of *Shipping Business* students achieved a distinction
- **77%** pass rate for *Dry Cargo Chartering* (43% global average across all Institute courses)
- **67%** average pass mark

A welcome chance to network and learn

International Open Days reveal breadth of Institute's offering

The Institute's Global Open Days held in September proved to be great opportunities for Members, students and potential students to come together across the world.

Most gathered online, although some people were able to attend Institute events in person, where it was safe to do so. During the sessions, guests had the chance to ask questions and freely discuss their study preferences/options, the shipping subjects that interest them, and the registration process.

Shipping industry newcomers as well as experienced professionals, current and potential students from many countries were invited to join and find out about gaining a professional qualification from the Institute.

The London and South East Branch met some old and new students on a visit to the Head Office.

The Pakistan Branch held a hybrid session where some participants were able to attend the event in person while others attended virtually. There was a good mix of maritime professionals as well as new graduates.

The newest branch in our network, the Netherlands Branch was in good company holding its Open Day online as the Canada, Middle East and Singapore branches also held their events online.

Meanwhile, the North East of England Branch held its Open Day at Stockton Riverside College, the local Institute Teaching Centre.

Last, but not least, the West Africa Branch held its Open Day in the auditorium of the Maritime University in Accra. It was a delight to see so many happy smiling faces. With some 85 students in attendance joining Fellows and Members supporting the celebration and answering lots of questions, it proved to be an uplifting day. Branch chair Frank Eshun FICS took the opportunity to talk to the students about the benefits of the Institute, its role within the shipping industry, and how to use the Institute to get ahead and to learn to stand out.

During the sessions guests had the chance to ask various questions. They were informed and guided on how to proceed and register for Institute examinations and pursue Institute qualifications, leading to membership.

The Open Days gave the Institute a great opportunity to introduce branch members to potential students. Attendants discussed their study preferences in connection with their academic and professional qualifications and their future career goals.

After some difficult few months, this latest series of Open Days provided many of the Institute's centres around the world an excellent and timely opportunity to meet once again.

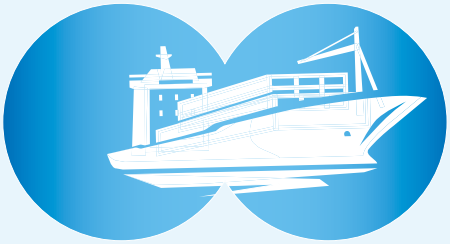
There is still plenty of time to talk through study options and to start studying with the Institute in this academic year. Candidates can take advantage of a free consultation service offered by the Institute Head Office in London. Contact education@ics.org.uk to start your professional studies in commercial shipping. ***SN***

London Branch


West Africa Branch

Pakistan Branch

The Open Days gave the Institute a great opportunity to introduce branch members to potential students"



View from the Wheelhouse

Consensus on conduct and confidentiality

Immediate past chair Susan Oatway updates members on Controlling Council outcomes

Susan Oatway

Over three days in October your Controlling Council (CC) met virtually for the Controlling Council 2021 meeting. The first two days were workshops on Governance and Finance before the meeting itself.

Day 1 was Governance and we started with a discussion on a Confidentiality Agreement (CA). Diligent readers will remember that earlier this year the CC agreed a Code of Conduct. The Agreement is the second piece of that work to bring our Institute into the 21st century with regards to the best practice for a modern, international organisation.

The CA has been put together by our Governance Working Group (GWG) and is designed to assist members on our Councils and Committee to fully understand their responsibilities in their roles. CC acknowledged that over the last few years we have had much greater insight into the personal data of Members, students, staff and contractors. It was also acknowledged that the ability to disseminate that information to a much wider audience than is proper is now far too easy. The GWG will be bringing this piece of work back to Council when all comments and suggestions have been discussed.

We then moved on to the other piece of work that the GWG has been doing, that of an organisational restructure. This is a huge piece of work and Members were keen to commend Nigel d'Souza FICS (Australia & New Zealand Branch) and YK Chan FICS (Hong Kong Branch) on all the work they have done. There are some very big themes around authority and responsibility, as well as the amount of work our volunteers do. This is an ongoing project and the CC will return to grapple with the ramifications next year.

Finance spotlight

Day 2 was all about Finance and the CC started with a discussion on membership fees. Every year your CC agrees minimal increases in fees, an average of 1.6% per year since 2000. This is less than inflation and has added to the increasing impact of costs on our Institute. It is not sustainable. Members had a long discussion about the value of fellowship, and its chartered status, and the comparisons of membership with other Institutes. Your branch representatives put a lot of thought into this proposal and there were concerns about membership retention and value, which is why the link between FICS and MICS, with regard to increase, is to be broken. There was an agreement that Fellows are further in their careers, have a particular value from their chartered status and that usually there is a degree of "wanting to make a difference" from them.

There was also significant discussion about membership retention and membership benefits and the Membership Committee has been further tasked with developing new ideas in that area. We all look forward to hearing more about this in due course.

The rest of the meeting was taken up with a discussion about the budgeting process, to aid understanding over the next year, and a presentation from the Finance and Audit Committee (FAC). The latter was concerned principally with outlining the FAC priorities for the coming year and aligning these objectives with the Head Office team. These include, but are not limited to, stabilising the Institute's finances to produce another profitable year, the formalisation of the Management Accounts process and improving branch reconciliations.

There was a sidebar discussion on an Internal Auditor and also what the Head Office does for the Institute of Chartered Shipbrokers Educational Fund (EF), a charity independent of the Institute that provides educational support for the shipping sector. I would direct all Members to the UK's Charity Commission website with regard to the EF: https://bit.ly/3qEtilC. I have written a number of pieces about the work done by the Fund and it was disappointing to realise how many members of CC had no understanding of this.

There were a lot of very positive comments from CC around the work done by the FAC in conjunction with the Secretariat. I would personally like to thank them all for their diligence in improving not only our finances but also the communication between both groups. It is only as we have started to pull together in the same direction that we have turned the ship around. Thank you.

The advantage of having two days of workshops before the actual meeting is that we get all the big discussions done in a positive way. It means we arrive at the meeting on the third day with a set of resolutions we know will have majority agreement. That is not to say we did not continue our discussions in the meeting, but the bigger themes were already in motion.

You should all be very proud of your branch representatives who gave up their time for three days to ensure that our Institute continues in the same positive forward direction. The draft minutes of the meeting will be shared as soon as complete with representatives and their branch committees. Please do engage with your local branch, or Head Office if you do not have a branch, if you have any questions about the proceedings and decisions taken.

This was my last CC meeting as chair, both of them virtual due to the pandemic, and I would like to thank my colleagues for their professional attitude, their diligence and their care of the Institute so it strengthens for the next 100 years. *SN*

New Institute leadership team steps up

The Institute officially welcomed its new team at October's Controlling Council meeting

Taking over the baton from Susan Oatway FICS as the new international chair of the Institute is Glenn Murphy FICS of the Ireland Branch who has been vice chairman of the Institute for the past two years. Working alongside Glenn will be Luis Bernat FICS, a former chairman of the Denmark Branch, who takes up the position of vice chairman of the Institute.

Glenn is a Fellow of the Institute with over 30 years' experience in international shipping working for both private and public sector bodies. He runs his own shipbroking firm based in Dublin and he previously served as a director of the Marine Institute and also on the Board of the National Maritime College in Ireland.

Kevin Shakesheff FICS, the Institute's 58th president, said that Glenn's knowledge and experience in the shipping industry will prove an "absolute asset" to the Institute at this time. "The Institute has emerged, after a difficult time, with a leader who will drive us forward and continue to develop the organisation into a global maritime Institute. My best wishes to Glenn Murphy and our new vice chairman Luis Bernat who like Glenn has a wealth of experience in shipping both in the UK and overseas. We are most fortunate to have two new officers with such excellent credentials."

Luis brings 46 years of shipping experience to the service of the Institute and is taking on his role as vice chairman with plans for united co-operation. "I am a firm believer in teamwork and joining Kevin and Glenn is of course in this spirit. I am looking forward to working with Glenn in his new leadership role and supporting the excellent work of the branches and all our Members."

Susan Oatway hands over the ceremonial chairman's medal to Glenn Murphy

Director of the Institute, Robert Hill FICS added: "I am eager to work with Glenn and Luis in maintaining the benchmark for professionalism in commercial shipping. I welcome their new thinking and look forward to making progress and serving the best interests of our Institute and our Members together." ***SN***

Aiming high with learning goals

Creating awareness, training and mentoring improves employability – strands that are pulled together by the Institute with its learning and networking offerings, according to South Africa Branch chairperson Catherine Moodie.

Interviewed for South Africa's *Freight News* publication, Catherine explained that job applicants today do not have the job-specific skills that are required and often lack work experience to perform the roles. "With the current global trend of digitising becoming more apparent in the shipping and logistics industry – along with the ability to adapt and be flexible – employees should be open to adapting their skills to the working environment with positive attitudes towards learning and meeting future changes," she said. "Many of the required skills are not available because of lack of training and the ability to adapt to the changes and keep shipping and logistics an attractive industry to work in."

She told *Freight News* that setting standards for both training providers and course material is essential and that qualifications need to have both local and international recognition. "This encourages employability and opportunities to grow within the industry," she said.

Catherine noted that a surge in online and distance learning courses over the pandemic has encouraged upskilling and has broken down barriers for training opportunities in the industry.

"Over the past 18 months there has been a growing need for online courses. Covid-19 restrictions and compliance required for the industry have created a need for digitisation of courses and the implementation of distance learning opportunities," she said.

Catherine highlighted the Institute's Understanding Shipping course and TutorShip distance learning programme as key tools in meeting those needs.

"As an organisation, we have seen a steady increase in interest from participants wanting to improve their skills and elevate their knowledge – especially with the changes we have experienced in shipping and logistics from recent worldwide events," she said. ***SN***

Shipping influencers join Institute ranks

The Greece Branch has successfully supported two shipping influencers to become Members of the Institute.

The first is Suzanna Laskaridis, a director at Laskaridis Shipping where she has been working since 2007. Ms Laskaridis has a Masters in Maritime Law from City University in London and is an active member of the Greek shipping community.

She is on the boards of the Hellenic War Risks Association and the UK Defence Club and sits on RINA's decarbonisation committee. Ms Laskaridis is also the general secretary and treasurer of the Aikaterini Laskaridis Foundation, a non-profit, cultural institution where she also heads and promotes environmental initiatives.

"Not only does she sponsor events and provide scholarships to her employees, but she also participates as a speaker at the Branch's conferences."

In 2016 she founded Real Time Graduates, a non-profit initiative that connects young graduates with valuable work experience within the maritime industry. Then in 2019, drawing inspiration from her experience in shipping and her environmental activity, she founded BlueCycle Greece, the first integrated company in Europe focused on the recycling of marine plastic waste originating from shipping and fishing activities.

Since 2018, Ms Laskaridis has also served on the Leadership Committee of the UN Sustainability Development Solutions Network. Crowning her achievements, in 2020 she was awarded the Next Generation in Shipping Award at the Lloyd's List Greek Shipping Awards.


Suzanna Laskaridis

In a letter of recommendation, the Institute's Greece Branch said Ms Laskaridis is a constant supporter of the Branch's teaching programmes and events. "Not only does she sponsor events and provide scholarships to her employees, but she also participates as a speaker at the Branch's conferences."

Also, through her Real Time Graduates initiative, she places young Institute students in internships at major Greek shipping companies. In return, the Greece Branch organises lectures for Real Time Graduates to promote the Institute's training programmes to maritime graduates.

In closing, the Branch said: "Ms Laskaridis is an inspiring shipping figure, and we expect that she will provide an added value to the Institute membership."


Aris Koropoulis

Extra supporter

Aris Koropoulis, managing director at Astra Shipmanagement, has also successfully been elected as a Member without examination under Bye Law 50.

Mr Koropoulis started his career as a broker at Eastern Mediterranean Maritime in 2006. He then joined Paralos Fund as an FFA analyst and gained experience of risk management. From 2012 to 2014, he joined the family business Thenamaris Ship Management as a chartering executive, becoming director of Astra Shipmanagement in 2014.

He is described as a "highly esteemed shipping practitioner" by the Greece Branch who recommended him for election. "He is a prominent figure in the shipping sector and has shown great dedication to the industry," the Branch said.

Mr Koropoulis is an active member of the Union of Greek Shipowners and regularly visits private and public schools around Greece to raise awareness of the seafaring profession and the shipping sector.

Specifically related to the Institute, he regularly participates at events and was a speaker at the Branch's 15th Annual Forum. He has also taught as a visiting lecturer for Dry Cargo Chartering and Ship Operations and Management at the Greece International Teaching Centre.

Additionally, Mr Koropoulis sponsors his company's employees to take their professional qualifying examinations with the Institute.

"We expect that Mr Koropoulis' input will help towards the promotion of the Institute's principles and ethics as he is continuously working to promote professionalism among the shipping community," said the Branch. **SN**

"He is a prominent figure in the shipping sector and has shown great dedication to the industry"

We congratulate and welcome the following who were recently elected to membership:

Newly elected members

Benjamin Hogan	Australia
Jasjeet Singh Kukreja	Australia
Nathan Crawford	Australia
Shardul Tiwatane	Australia
Edson Augusto Haniel Vegi	Brazil
Igor Skotnytsky	Canada
Sven Bornemann	Chile
Antonia Petrou	Cyprus
Elena Ppeli	Cyprus
Mikaella Stavrou	Cyprus
Anna-Sophie Schauer	Germany
Athina Chrysomalli	Greece
Athina Mangirou	Greece
Capt. Konstantinos Pantos	Greece
Christos Argyros	Greece
Dimitrios Dimtsas	Greece
Dimitrios Ntzouras	Greece
Dimitrios Sakkas	Greece
Dimitrios Tsoumanis	Greece
Eleni Tsepopoulou	Greece
Elisavet Stavridi	Greece
Evgenia Smyrli	Greece
George Neratzoulis	Greece
Ilektra Mantzikou	Greece
Ioannis Kavouras	Greece
Iphigenia Grigoriou	Greece
Kalliopi Konte	Greece
Konstantina Afali	Greece
Konstantinos Kavaliotis	Greece
Kyriaki Lekodimitri	Greece
Maria Tzigianni	Greece
Marina Tzouganatou	Greece
Nick Papadopoulos	Greece
Nikalaos Karagiannis	Greece
Nikolaos Stamatopoulos	Greece
Nikolaos Theodosiou	Greece
Nikolaos Valtas	Greece
Olga Nikitina	Greece
Pericles Paronis	Greece
Persefoni Sakellaridi	Greece
Prifti A Marios	Greece
Raphael Spyridon	Greece
Sotitirios Alogakos	Greece
Styliani Malli	Greece
Theodore G Katsaris	Greece
Vasileios Iliadis	Greece
Vassilios Stavropoulos	Greece
Vrettos Moulos	Greece
Xeni Petrogianni	Greece
Shijin Li	Hong Kong
Kyle Carey	Ireland
Caroline Wainaina	Kenya
Diana Businge	Kenya
Emre Inandi	Netherlands
Fangfang Jia	Netherlands
Fatme Shaban	Netherlands
Hubert PM van Wijngaarden	Netherlands
Kathy Schiere	Netherlands
Adeyemi Anthony Adeniyi	Nigeria
Manohar Jobanputra	Nigeria
Ola Felix Alabi	Nigeria
Olwaseye Adewole	Nigeria
Gabriel Moises Fuentes Lezcano	Norway
Goncalo Barreiros	Portugal
Rama Krishnan	Qatar
Alexander Romanov	Russia
Anna Pekhova	Russia
Amardeep Grewal	Singapore
Amy Kilmer	Singapore
Debbie Neo	Singapore
Esther Eng	Singapore
Faizudeen Saifudeen Mohamed	Singapore
Jenny Octavia Tjuwita	Singapore
Karan Makin	Singapore
Lekshmi V Salvady	Singapore
Lim Ming Lian	Singapore
Peck Yi Ping	Singapore
Peter Robertson	Singapore
Sudev Raja Naran	Singapore
Tan Heng Shoon	Singapore
Wong Hui Mei	Singapore
Kanchana Bopitiya	Sri Lanka
Lasantha Manohara Muniratne Wedige	Sri Lanka
Maleena Awn	Sri Lanka
Nirmal Dissanayake	Sri Lanka
W Anushka Namal Kumaradasa	Sri Lanka
Claes Gunnerson	Sweden
Alexey Mudragelya	Ukraine
Anitha Dmello	United Arab Emirates
Shailesh Madelkar	United Arab Emirates
Anthony Kokkinis	United Kingdom
Capt. Tushar LR Potey	United Kingdom
Jonathan Trish	United Kingdom
Katrina Ross	United Kingdom
Kristofer Karlsen	United Kingdom
Maria Carmen Guerra-Prados	United Kingdom
Steven Windram	United Kingdom
Bahadir Unal	United States
Marvin Machridza	Zimbabwe

Promoted to Fellow

Kyaw Myo Win	Myanmar
Aderemi Louis Oyedele	Nigeria
Michael Oyewo	Nigeria
Daminda Mulgama	Sri Lanka
Manoharan Suloshana	Sri Lanka
Mohammed Firoz Abdul Lathiff	Sri Lanka
Sachithra Dissanayaka	Sri Lanka
Franca Maturo	Switzerland
Innes Macleod	United Kingdom
Robert Merrylees	United Kingdom

Re-elected to membership

Kristina Daus-Petersen	Denmark
Tamunotonye Saramaduo Hart	Nigeria
Vishal D Bajpai	Singapore

Bye-laws 50

Aris Koropoulis	Greece
Souzana Laskaridi	Greece

Build a virtual community

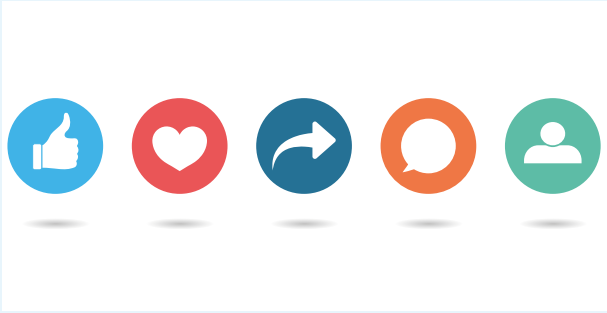
Gertrude Adwoa Ohene-Asienim urges Members to tag, like, click and share

Gertrude Adwoa Ohene-Asienim

The global Institute and many of its branches have made great efforts to create and sustain online content and have made use of social media – a powerful tool to keep people connected and a way of receiving or sharing information in real time – to increase the reach of the Institute. Social media is also the fastest, easiest and one of the most cost effective ways of connecting with each other. Recently, when some social media platforms went down for hours, the world was in turmoil. Once it was taken away, albeit for just a few hours, I realised how addicted we have all become in one way or another to social media. Your Membership Committee is therefore asking the question, how can we then explore this to our advantage as an Institute?

With current global trends, the world is getting more digital. Our Institute is truly global with branches in 26 different locations and non-branch members in many other countries spread across the continents of the world. We can expand our reach and network by connecting and staying connected through creating relevant content, sharing information on happenings in our branches and continents, and by visiting our social media pages more frequently to tag, like, click and share information of interest. In so doing we will create traffic on our pages and make the Institute more visible to others.

I am therefore inviting you to subscribe and join the Institute Members only LinkedIn, Facebook and Instagram pages. Tag, like, click and share Institute news on your individual social media pages. Share branch information, events, webinars, election of



new chairman and committee members, awards to students and many more stories of interest with us.

We also want to celebrate the achievements of our Members across the globe, information we might never have known without these tools. Send us your most recent interesting news, milestones achieved in shipping, and your current global and unique appointments, and we will celebrate with you.

Through this simple act, we will not only stay connected but receive information in real time, have fun, build, and enhance our brand, and create awareness about our Institute to give us the needed recognition we are all looking for.

I am counting on you to make this happen. Together we can! **SN**

Gertrude Adwoa Ohene-Asienim FICS is chairman of the Institute's Membership Committee. She can be contacted via membership@ics.org.uk.

Fond farewell to London stalwart

At the London & South East Branch AGM in October, the Branch said thank you and goodbye to a long-standing committee member, Michael (Mike) Harrison FICS. Mike became a committee member of London Branch (as it was originally called) in 1981, and during his time, he has been involved in all aspects of the Branch's committee work. Most recently he has been the Branch's secretary, ensuring that events are correctly organised, various dates are adhered to, and ensuring the Branch acts within its bye-laws. At the same time, he has acted as the Branch's treasurer, keeping a tight handle on finances, while ensuring the Branch delivers its accounts correctly.

Previously he was involved in the pilotage committee for the Institute, was a former chairman of London and South East Branch, and was the Branch's Controlling Council representative until January 2018. Chris Hibbert, chairman of the Branch, said: "It would be appropriate to say that Mike has been a fixture and fitting on our committee."

"We were delighted that our London International Shipping Week 2021 (LISW) Branch seminar, for which he was the prime organiser, enjoyed great success as our first LISW online event. With help from our branch committee members, he developed and created the programme, the title, and persuaded speakers to join us. On our behalf I would like to thank Mike and all who helped to create and deliver this wonderful seminar."

After 40 years, it goes without saying that the Branch committee will miss Mike. He has kept the committee on the straight and narrow, helped it to find solutions to problems, always been available on the phone, and been a constant figure at all events whether social or educational. Although he is stepping off the committee, he assures the chairman that he is still planning to attend events, and the Branch will welcome him with open arms.

Mike was honoured to receive the Shipbroker's Medal

The Branch presented an engraved tankard to Mike, and he has confirmed that it will be well used. In addition, the immediate past chairman of the Institute, Susan Oatway FICS, also made a presentation to Mike, of a Shipbroker's Medal in recognition of his long-standing commitment and support.

The Institute presents the Shipbroker's Medal to only those Fellows who have given above and beyond in their support of the Institute. This is certainly true of Mike.

The Shipbroker's Medal was awarded to Mike in recognition of all of his work at branch level supporting both members and students in London for over 30 years. Susan said: "It is a great honour to give Mike the Shipbroker's Medal for his long service to the Institute. He joins a very select band of Fellows who have been given this honour and it is richly deserved." ***SN***

Shanghai's successful two-week development course

The Shanghai International Teaching Centre hosted its popular Classical Shipping Development Program in August, welcoming 34 candidates from 22 well-known companies.

The students enjoyed the development programme

Susan Oatway FICS, immediate past international chair of the Institute, lectured for the sixth time on shipping business and dry cargo chartering.

Dr Fan Wei, vice president of Skuld, talked about charterparties and damages, insurance, law and unsafe ports. Shipping experts Ji Wen Yuan, chairman of Seamaster, and Andrew Meadows, vice president of Skuld Hong Kong, shared their experience with the attendees.

The programme was offered in a hybrid format, with tutors and experts giving lectures and interacting with students through an online platform accompanied by an in-person award ceremony and drinks reception.

Liu Xiao Dan, vice director general of the shipping office of Shanghai Pudong New Area, presented the end-of-programme certificates which are jointly issued by the Institute and the Professional Qualification Authority of the Ministry of Transport of the People's Republic of China.

Anni Wang was honoured as the "Best Candidate" for the 2020 training program and received a scholarship, while Ma Chan, who has completed her professional qualifying exams, received the 2020 Institute China Prize. ***SN***

Running for education

North East of England Branch chairperson Gillian Clark decided to take addressing the Branch's shortage of funds into her own hands earlier this year.

The pandemic had meant that the Branch was unable to hold key social events, including two revenue-earning annual dinners.

Gillian embarked on a strict training programme to undertake an ultra marathon over two days from Carlisle to Newcastle, a distance of 70 miles over rough terrain through the Lake District.

Gillian raised a total of £1,240 which she kindly donated to the Branch. It was a fantastic effort and one that enabled the Branch to keep its head above water through the pandemic.

The Branch would like to say a heartfelt 'well done' to Gillian for her amazing achievement.

The Branch is also congratulating its vice chair and education officer Nikki Sayer FICS who has been recognised for her work in education, shipping and customs.

Nikki was presented with the Breaking the Mould Award at this year's Tees Businesswomen Awards 2021.

The award, sponsored by local firm Steel Benders UK and presented by its managing director Tania Cooper, recognised Nikki's ongoing work in the region. *SN*

Gillian (middle) crosses the finish line after a 70-mile ultra marathon

Nikki, left, receives her Breaking the Mould Award

Pride in student's achievements

The West Africa Branch has expressed its sincere pride in one of its students, who registered for five subjects in the latest exam sitting and passed all with distinction.

Adewole Oluwaseye Mayowa said he has a passion for the development of the industry, especially in Africa, and used the opportunity of the pandemic to start his professional qualifying exam journey with the Institute.

He said he is "delighted" to have passed all his papers within one sitting, especially in a year that was both physically and mentally draining.

Adewole said he looks forward to a future characterised by rapid change in regulations, standards and the environment and to the deepening of financing and financial services available to Africa.

"In particular, I look forward to what these gains will add to the expansion and growth of our great Institute; opportunities for our esteemed professionals and our maritime students who are eager to build a career in our industry." *SN*

Adewole 'delighted' at passing all five exams with distinction

Fellow presented with Institute badge

Immediate past international chair Susan Oatway FICS took the opportunity at an Awards ceremony in London to present a long-time Fellow with the Institute pin.

Susan attached the pin to the lapel of Kyriacos Panayides, managing director of multipurpose ship operator AAL Shipping.

Both Susan and Kyriacos were guests at the Heavy Lift Awards at the Royal Lancaster Hotel, London, in October. *SN*

Susan presented the Institute token

Celebrating chartered mariner success

Institute Fellow Capt SM Ajmal Mahmoodi has been honoured as Pakistan's first chartered master mariner by the Honourable Company of Master Mariners.

In a ceremony onboard HQS Wellington, the headquarters of the Honourable Company, Capt Mahmoodi's dedication to the maritime profession was recognised. He received his award from Commander Les Chapman CMMar FNI, Royal Navy UK.

Chartered status is granted to qualifying Master Mariners and recognises exceptional service. It is considered a mark of excellence that evidences personal eminence and expertise, competence and peer-recognised qualities.

Capt Mahmoodi's engagement in the industry was described by the Company as "almost second to none". His career highlights include establishing a Nautical Institute branch in Pakistan in 1987 and establishing the Maritime Training Institute in Karachi in 1998. He is also the current vice president of the Nautical Institute. ***SN***

Capt Mahmoodi paid a visit to Head Office while in London

Cyprus celebrates IMO World Maritime Day

The Cyprus Branch organised a networking event in Limassol on September 30th to celebrate the IMO's World Maritime Day.

The event was honoured by the presence of members of two collaborative organisations, Wista and Youngship Cyprus.

Christina Christoforou, chairwoman of the Cyprus Branch, noted in her speech that the day was devoted to the seafarers who are facing unprecedented hardship due to Covid-19 pandemic.

The President of Youngship Cyprus Antonis Varnava also underlined that seafarers are the key workers for global supply chains and that the Covid-19 pandemic has placed extraordinary demands them.

Wista Cyprus spokesperson Marilena Morphaki said this year's World Maritime Day will put the spotlight on other issues related to the human element of shipping, including the safety and security of life on board ships, seafarers' wellbeing and the importance of ensuring an appropriately trained and qualified workforce, ready to meet the challenges and opportunities of digitalisation and automation.

The Branch chose to support The Mission to Seafarers in Limassol at the event and handed over a cheque to the local chaplain Ken Wiseman after the event. The donation will go towards delivering care boxes, simple everyday things that seafarers need but cannot purchase themselves.

Speeches were also given by Natalia Margioli FICS on behalf of Greece Branch and Elina Kassotaki FICS on behalf of Wista Hellas.

The Branch took the opportunity to honour the immediate past chairman of the Branch at the event, Yiannis Shittas, presenting him with the Institute medallion. The medallion was presented to Mr Shittas by another ex-chairman of the Branch, Andreas Andreou. ***SN***

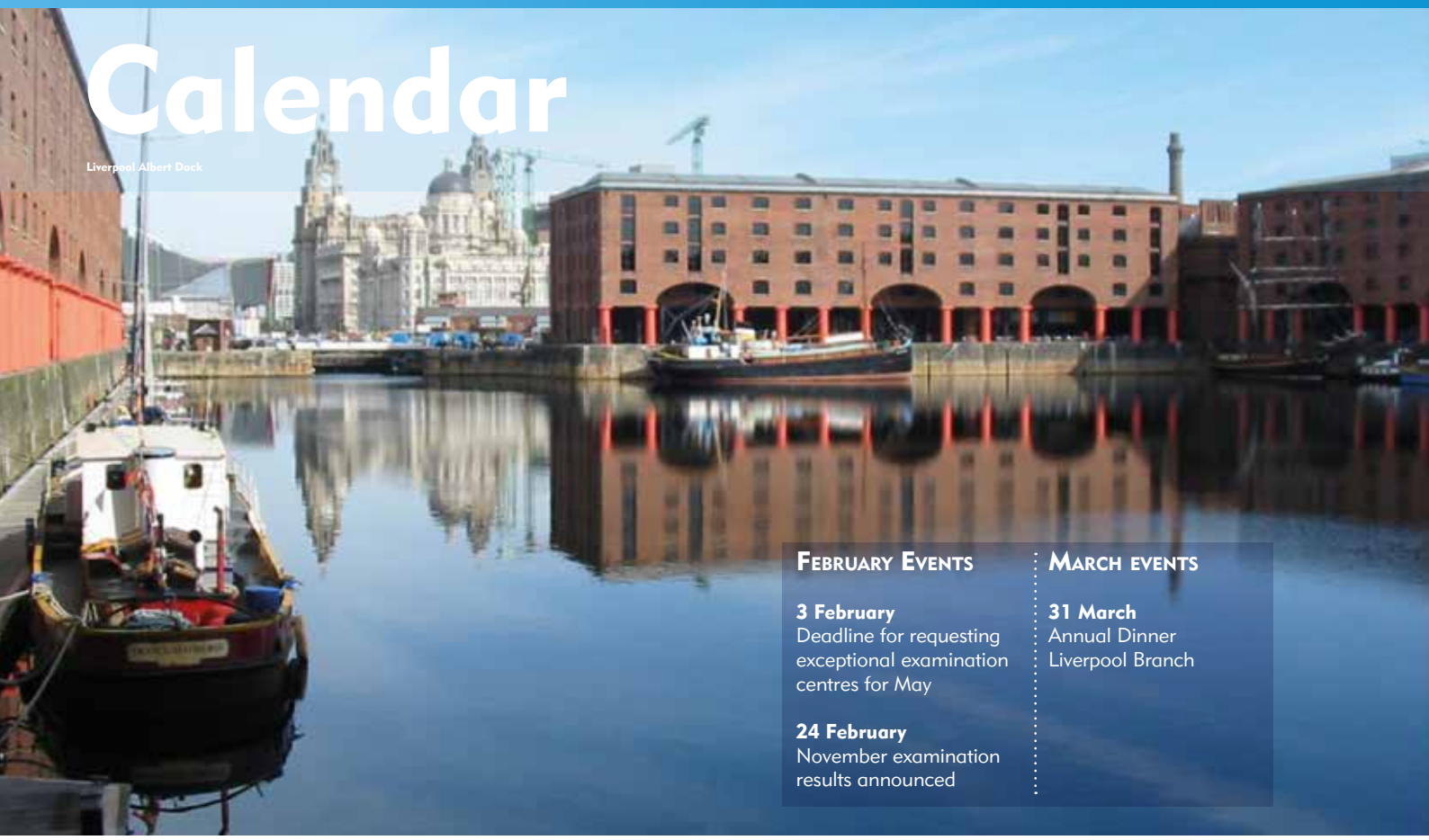
The Branch presented a donation to the local Mission to Seafarers

Spreading the Institute word

The Cyprus Branch supported the Thalassa 2021 – meaning 'Sea 2021' – in Limassol in October, an event organised by the Deputy Minister of Shipping and the Mayor of Limassol.

The Branch kiosk was staffed by the Branch chair, Christina Christoforou FICS, and the Branch vice chair, Stavros Kavalierakis FICS. A few guests came to visit and the Branch looks forward to welcoming them as new students in the near future. ***SN***

Calendar



Liverpool Albert Dock

February Events

3 February
Deadline for requesting exceptional examination centres for May

24 February
November examination results announced

March events

31 March
Annual Dinner
Liverpool Branch

Institute Annual General Meeting

The Institute of Chartered Shipbrokers held its Annual General Meeting (AGM) on October 7. Nine members attended in person in the Institute's office and another 114 joined online. This was once again the largest attendance at an Institute AGM for many years and it was wonderful to see an increasing number of members from around the world taking an interest and participating in the AGM.

The president welcomed all those attending and commended the director, Head Office staff and the Finance and Audit Committee for returning a profit in 2020-21. He also acknowledged Susan Oatway who completed her term as Institute chairman. She in turn thanked everyone for their support during a challenging two year term.

The annual accounts for the year ending May 31, 2021 were presented to the meeting and discussed. Members took the opportunity to ask questions about the impact of the pandemic on the Institute finances and the forecast for the coming financial year.

The AGM continued with the formalities of confirming the composition of Controlling Council for 2021-22, subject to all Controlling Council representatives signing the newly introduced Code of Conduct which is applicable to all Council and Committee members. The AGM also re-elected haysmacintyre as auditor for another year.

The president thanked all members for attending and contributing to the AGM. *SN*

Institute director Robert Hill, president Kevin Shakesheff, and past chairman Susan Oatway answered questions at the AGM

The Secret Broker

Fear of missing out

FOMO – fear of missing out – is a syndrome not confined to anxious teens in the pitiless grip of social media. With the market running as hot as it has been in recent months, I am gripped by the usual panic that deals are shooting passed me that I should be able to land.

All brokers are afflicted by the same sickening sinking feeling when they hear that a client has concluded business without them. However, the classification of what constitutes as a client needs to be more closely defined.

There are clients who I regularly do business with. They know what I can do, and I know what they expect. They have paid for my house. It hurts if they do deals with others. But the house is paid for. And there are clients I have known for decades – we have analysed every market turn together, discussed a myriad of investment strategies. Away from the office we have regularly broken bread together, over the years eaten shoals of fish, and drunk vats of wine. I have met their wives, their children, patted their dogs. And yet concluded no business. Are they clients after a decade or more of effort without a penny of commission to show for it?

They will do relatively few deals, many years apart, and one has to be realistic about the chances of a pay-out. I only talk to them because I like them and they understand that as I feed them with information, so they feed me. They see brokers as pollinators – carrying information and gossip around the market in a mutually beneficial process.

Occasionally they will pop up and do business. It happened to me a couple of years ago – twenty years without a deal, followed by a newbuilding mandate and an exclusive purchase enquiry. Patience and Tenacity should be every broker's watchwords.

And then there are clients who are clients only in the sense that you know them. They will answer your call but there is no real connection and if they come to a ship I control via another broker I am neither surprised nor concerned.

But while desiring this man's art and that man's scope, I can't complain. It has been a modestly productive year and I have a few units still to deliver. I have a bulk carrier to deliver next week that was entirely negotiated in my absence. Two of my colleagues picked up the threads and tied together a deal while I was on holiday with zero input from me during the negotiations. I am eternally grateful to them both.

Countless family holidays in the past have been poisoned by a running negotiation. There was a period when mobile phones were able to catch you almost anywhere while broadband was unknown. You could be disturbed on holiday but be virtually helpless in managing the deal.

While I have forgotten the name of every wretched vessel I have negotiated on holiday, I will never forget the frustrated little faces in the rear-view mirror as we sat locked in the car at the beach while their desperate father made another phone call. *SN*

the stern

No time to fly

DHL – the official logistics partner of the James Bond *No Time To Die* movie – took a precious cargo of 007's cars on an epic sea journey in September.

The freight forwarder delivered eight original James Bond vehicles for exhibition from the UK to the US, including Bond's iconic silver-grey Aston Martin DB5.

The vehicles were moved from Norwich, Norfolk in the UK across the Atlantic to Los Angeles, US and will be the main attraction of an exhibition at the Petersen Automotive Museum.

The cargo contained five Aston Martins, two BMWs and one Lotus Esprit S1, known to fans as *Wet Nellie* from *The Spy Who Loved Me*.

"We are incredibly proud of the support DHL has provided the last five James Bond films. To pull off a feat of this magnitude and guarantee a smooth process across national borders requires the collective effort and orchestration of our international DHL network and its respective teams," said Monika Schaller, executive vice president of corporate communications, sustainability & brand. **SN**

Bond's iconic silver-grey Aston Martin DB5 was among the cargo delivered

Elves take to the skies

With the focus on a predicted scarcity of turkeys and toys this December, another worrying festive shortage has surfaced. Elves are said to be in short supply – so short in fact that 300,000 have been air lifted to the UK to avoid congested ports and shipping delays in China.

Thankfully these are not Santa's elves – although there are concerns that isolation and quarantine might impact staffing at the North Pole.

The Elves Behavin' Badly dolls have been hit by the double whammy of high demand and low shipping availability, which has created a stock deficit.

The company behind Elves Behavin' Badly, PMS International has turned to air freight for 300,000 dolls to meet demand in the UK.

A number of major retailers sold out in 2020, even without the shipping issues, so consumers may experience difficulties getting their hands on the dolls this year.

The mischievous dolls were launched five years ago and have proved very popular, spreading mayhem in homes throughout December.

Shipments of Elves to locked-down Australia have doubled this year and a retailer there has also enquired about airfreighting, said the company.

PMS has reported less problems with deliveries to the US, Europe and Scandinavia where 95% of orders had already been shipped by early November.

Shipping Speak

"Shipping is the physical equivalent of the internet and much like the internet we are truly at sea when it goes down."
Alderman William Russell, Lord Mayor of the City of London, UK

"Regionalisation will lead to retaliation which will lead to complexity and a more expensive supply chain."
Soren Toft, CEO, Mediterranean Shipping Company (MSC)

INSTITUTE OF CHARTERED SHIPBROKERS

Want to learn about shipping?

The Institute of Chartered Shipbrokers has you covered

As a truly international provider of professional maritime training, the Institute of Chartered Shipbrokers offers an unrivalled programme of education and qualification.

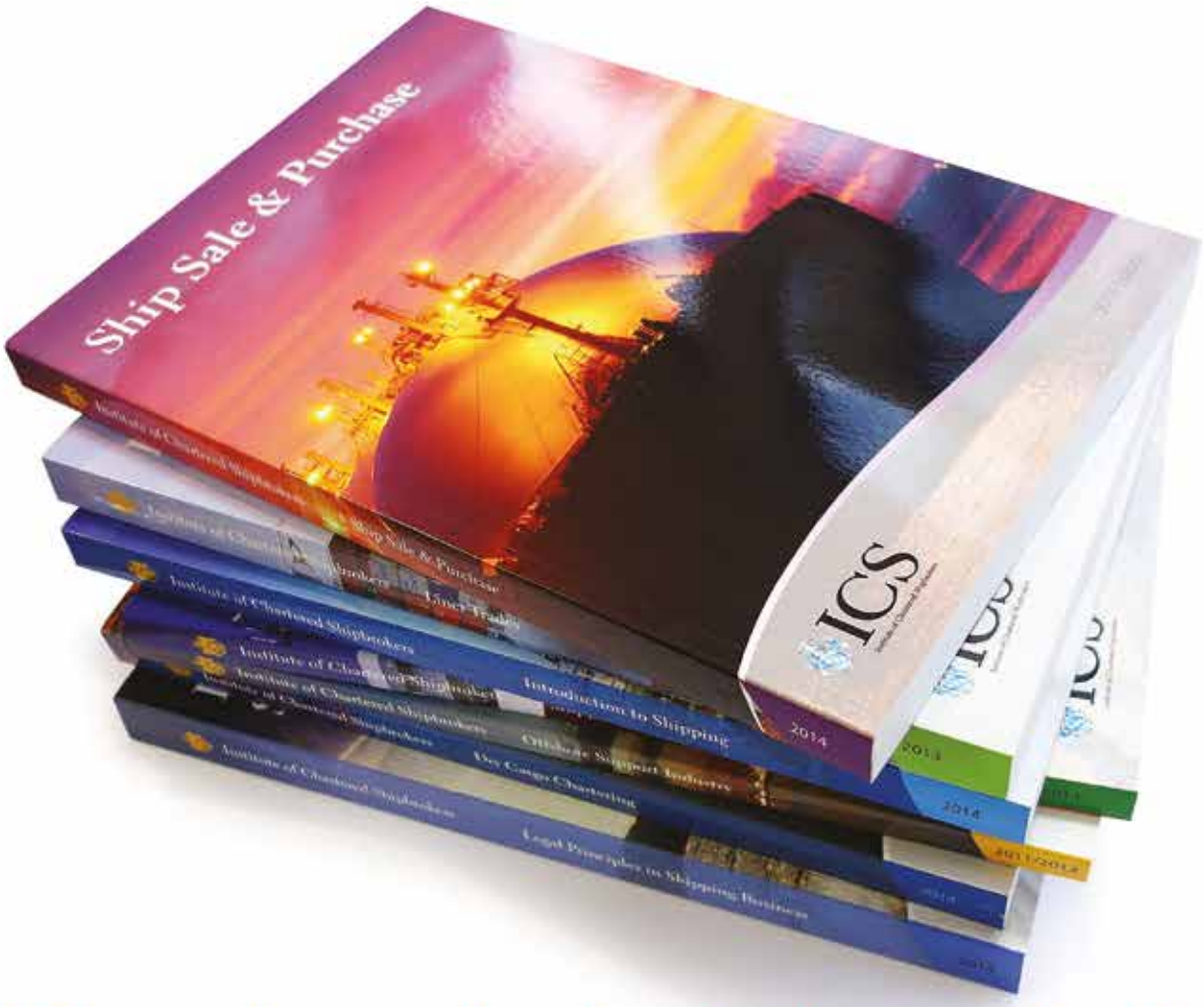
The Institute offers one-day introductory courses through to professional qualifying examinations leading to membership and chartered status.

While the Institute's maritime induction courses offer a tailored introduction to the maritime world for industry newcomers, diplomas allow specialism in a number of different areas, including ship operations, tanker chartering, port agency, shipping law and marine insurance.

At the highest level, the Institute's professional qualifying examinations represent the route to membership, allowing individuals to join the Institute's international network of brokers, forwarders, agents, managers, insurers, lawyers and other shipping service providers. Membership commands respect, demonstrating a commitment to lifelong learning. It also opens the doorway to an established and worldwide network within the shipping industry.

Wherever you are in the world, find the right Institute of Chartered Shipbrokers' professional development option for you and contact the Institute to start your journey today.

Contact the Institute on education@ics.org.uk or on +44 (0)20 7357 9722



Written by professionals for professionals

Shipping has become more complex to the extent that the name shipbroker, which at one time was thought to apply only to those engaged in chartering dry cargo tramp ships, now embraces separate disciplines in tanker chartering, ship management, sale and purchase, port agency and liner trades.

As an independent international professional membership organisation, the Institute of Chartered Shipbrokers strives to promote a world class program of education and training to ensure that all its members are knowledgeable about their business. As a result, the Institute produces and publishes a comprehensive series of books on shipping business.

The Institute's sixteen books are unique in that they have been written by professionals for professionals in the shipping industry. They now undergo a regular review where they are peer reviewed, revised and updated by professionals in their particular discipline and peer reviewed again, so that an accurate revision can be achieved.

The books themselves will continue to be part of the TutorShip course, but our goal is to make them more widely available to the general shipping industry, which has long requested our books as general reference titles.

Members are entitled to a £45 discount on all of the Institute's publications.

To place an order, please complete a book order form and return it to us.

For book order forms and support, please visit: www.ics.org.uk/learning

Members receive a £45 discount on all books

INSTITUTE OF CHARTERED SHIPBROKERS