COMPREHENSIVELY YACHTS
HFW YACHTING INDUSTRY BRIEFING

With 2023 drawing to a close, it has been another busy year for HFW's yacht team and we are delighted to present the latest edition of Comprehensively Yachts, which you will find packed with topical comment and analysis.

Twenty one months since the invasion of Ukraine, the yachting industry, having been hard hit by the economic impact of Russian sanctions, has largely settled down and found new business to replace that lost or turned away. However, the risk of an inadvertent sanctions breach remains for those not taking care when onboarding new clients and accordingly we start with a look at the current sanctions landscape from our market leading sanctions team, together with a round-up of some of the high profile ongoing legal challenges.

Next, our marine insurance specialists consider whether the widely used American Yacht Form R12 is still fit for purpose or whether the time is right for the marine insurance industry to move on to a bespoke wording better suited to English law and the practices of both the London insurance market and the modern yachting industry.

The possibility of anonymously enjoying beautiful places in the company of your friends and family from the privacy of your yacht is key to the allure of yachting. However, with AIS technology enabling everyone with a smart phone to know your yacht's every move, the temptation to turn off a yacht's AIS transmission and "go dark" is real. Our admiralty team explore the law behind the transmission and how, if at all, you might achieve an ex-directory status.

Our Paris office reports on a recent land-mark conviction of the captain of a 26 meter yacht by the Maritime Court of Marseille following his repeated anchoring in protected posidonia meadows and the threat such conviction has for the wider yachting industry.

Finally, we round out this edition with a long read on Cyber Security, the increasing regulation around it and the growing need to take it seriously.

We hope you enjoy this edition and please do keep in touch. If there is anything you would like us to discuss in forthcoming editions, please do let us know.

WILLIAM MACLACHLAN
Partner, London
T +44 (0)20 7264 8007
E william.maclachlan@hfw.com

Sanctions Update

As sanctions measures targeted at Russia expand and evolve around the world, yachting industry suppliers and service providers remain heavily exposed to the risk of a breach. All such businesses should continue to carry out thorough due diligence on the yachts they service as well as their registered owners and ultimate beneficial owners, to determine whether they are dealing with either a sanctioned person or a person who falls within the wider category of persons connected with Russia.

We have seen a recent focus in the UK on the concepts of ownership and control, with indications that the English Courts will construe UK legislation in a way which potentially increases the impact of UK sanctions measures. The US continues to take steps to enforce its sanctions, and we are seeing the US and other authorities look carefully at the measures which might be adopted to move beyond the temporary freezing of assets, towards the permanent requisition and seizure of such assets. The EU is actively considering its 12th package of measures against Russia, which is expected to be adopted before the end of 2023.

There have of course been several high-profile actions relating to yachts with a Russian connection.

In the UK, PHI (a yacht owned by Russian property developer Sergey Naumenko) is still being detained by UK authorities after a failed challenge against their decision to seize the yacht. Naumenko's attempt to argue that a lack of political connections rendered the seizure disproportionate failed in the UK's High Court, which found that the UK Government had the right to seize the yacht on the basis that it was owned by a person connected with Russia. The Court further found that a Russian-owned vessel does not need to be owned by a sanctioned person or a person connected with Vladimir Putin in order to be lawfully seized in the UK. We are likely to return to the PHI in the new year, as we understand that the case has been appealed to the Court of Appeal.

In the US, matters related to the seizure of the yacht AMADEA continue, with Eduard Khudainatov, a Russian businessman, filing a claim on 28 November 2023 before the US District Court arguing that he *"is and has always been the ultimate beneficial owner of"* the AMADEA and challenging the US Government's seizure and forfeiture of the yacht, which had been based on their belief that the yacht is owned by Suleiman Kerimov, who is under US sanctions.

The proposed sale of ALFA NERO to Google CEO Eric Schmidt has fallen through after Schmidt withdrew his bid. Authorities in Antigua and Barbuda had seized the yacht, claiming it to be owned by sanctioned Russian billionaire Andrey Guryev. However, Mr Guryev's daughter has claimed to be the sole beneficiary of the trust that owns the yacht and, thus that she is the ultimate beneficial owner of the yacht and not Mr Guryev. Her appeal against the decision to sell the ALFA NERO has been dismissed and a corresponding injunction application has been refused. The Antiguan authorities still intend to auction off the yacht and maintain that it has been validly seized.

Elsewhere, the NORD, a yacht owned by Alexey Mordashov, continues to attract attention as it circumnavigates the world whilst keeping out of reach of western sanctions. In October 2023, it was spotted in Hong Kong before then proceeding to Cape Town.

DANIEL MARTIN
Partner, London
T +44 (0)20 7264 8189
E daniel.martin@hfw.com

STEPHEN GREEN
Associate, London
T +44 (0)20 7264 8346
E stephen.green@hfw.com

“The R12 wording is popular due to it being an all risks policy and because it seeks to address some of the unique characteristics of running and managing large yachts, as opposed to commercial ships.”

R12 Yacht Wording: Time for Something New?

As we reach the end of the year, many yacht owners and managers will be starting to think about insurance renewals. For many years, the majority of large yachts have been insured either on the basis of the American Yacht Form R12 or the London Institute Time Clauses Hulls. The latter is aimed at commercial shipping and has to be heavily adapted for the yacht market, but it does have the advantage of being well used and understood in the marine insurance market.

The R12 wording is popular due to it being an all risks policy and because it seeks to address some of the unique characteristics of running and managing large yachts, as opposed to commercial ships. However, it has a number of features which, at best, are hard to understand and, at worst, are seriously problematic for both insurers and assureds. Throughout it is drafted in the tenor and from the perspective of US law and practice, with concepts and approaches often not found in English Law. For example:

- There are references to the need to file a *“sworn proof of loss”* as a requirement for any claim being brought against the insurer.
- The same clause goes on to require all evidence in support of that loss to be provided within 90 days; something that will often be impossible to achieve.
- The wording refers to *“examination under oath”*, a concept that is not readily understood under English law.
- In section F there is a long clause entitled *“service of suit”* which makes express reference to the service of legal proceeds in the USA.
- The proceeding section E deals directly with US federal longshoremen’s cover, which is unlikely to be of relevance to the majority of larger yachts.

There are other places where the wording does not readily integrate with other London market standard wordings, for example around the war exclusion, the treatment of deductibles, the return of premium and cancellations. It also contains a very short time limit of 1 year for bringing claims (though this is often amended to 2 years by agreement). Even where amended, this remains a very short time period and outside of standard market practice in the marine sector.

The are positive elements to the wording. From an assured’s point of view, the “no waiver” in the sue & labour clause is useful and would likely preclude an insurer from arguing that the assured had taken steps which were contrary to a notice of abandonment in the event of a potential constructive total loss. It also seeks to deal with launches and tenders head on and actively include them within the scope of the insurance.

However, in the round we consider that the market would welcome a bespoke yacht wording for property insurance. The yacht market has moved on considerably since the R12 entered common use, with ever increasing values, complexities and liabilities. A modern wording which reflects current market practice and the requirements of sophisticated yacht owners would only be a positive development.

ALEX KEMP
Partner, London
T +44 (0)20 7264 8432
E alex.kemp@hfw.com

JENNY SALMON
Legal Director, London
T +44 (0)20 7264 8501
E jenny.salmon@hfw.com

Is complete anonymity a Holy Grail for yacht owners?

There are many reasons why a yacht owner might want to make their yacht “ex-directory”. For example, to preserve the identity of the yacht in circumstances where the owner and/or his guests may be of interest to the media or where it is operating in a hostile environment. Such status would no doubt be very popular if it was achievable. As always, however, there is a fine line to tread between ensuring anonymity and complying with national and international rules and regulations and every yacht owner and captain must consider the position carefully.

The starting position under SOLAS[1] Chapter V, Regulation 19.2.4, is that “all ships” of 300gt and upwards, engaged in international voyages must have an automatic identification system (AIS) enabled. There are nuances when it comes to the application of these rules to yachts, but most large yachts carry AIS transponders and receivers and use them, whether mandatory or not.

A vessel’s AIS transponder operates using VHF frequency radio waves, in the same way as a VHF radio and has about the same range as a VHF radio. Vessels within range of an AIS transponder should be able to pick up its AIS transmissions on their AIS receivers. In addition, a global network of base stations and satellites also pick up AIS transmissions. Around the UK alone, there are over 60 base stations receiving AIS data from passing vessels.

The AIS databases source data from shore stations, satellites and even other vessels. Certain companies, such as MadeSmart, maintain their own database and harvest AIS data from vessels fitted with their fleet tracking equipment. As the vessels fitted with fleet tracking equipment circumnavigate the world, they capture and upload AIS data from passing AIS transponders. The databases then further supplement this data by purchasing additional data from each other and other sources. Service providers such as Marine Traffic and Lloyds’ List purchase the compiled data and use it in their products.

For a vessel for which maintaining an AIS transmission is mandatory, turning off its AIS transmission is going to land that vessel’s owner in trouble with the law unless it is able to rely on one of the available exceptions. The IMO guidelines (SOLAS Resolution A.1106(29))[2] require a vessel’s AIS to be in operation whenever underway or anchored. The only exception to this rule is when:

- the vessel is in imminent danger;
- the vessel’s captain is certain that maintaining the signal broadcast will compromise its safety and security. In such case, he/she must record the incident in the unit’s logbook and file a report to the competent authority, including a valid reason why he/she has decided to switch the AIS off, as well as the other measures taken; or
- the “silent mode” is operated in dangerous waters (for example, the suspected presence of armed pirates). However, this should be temporary and the AIS should be switched back on as soon as the threat is no longer considered imminent.

1 The Convention for the Safety of Life at Sea: SOLAS (imo.org)
2 A 1106 29 (imo.org)

A desire to remain anonymous because you don't want the press to be able to track you does not fall into any of the exceptions set out above. Further, the general presumption from the competent authorities, banks, insurers and others is that if a vessel is operating "dark", i.e. with its AIS switched off, then it may well be participating in illegal activities. This may ultimately draw more attention to the vessel than leaving the AIS turned on.

In most cases, therefore, you cannot lawfully turn off your AIS transmission. So how else might an "ex-directory" status be achieved?

Some have suggested blocking individual websites from receiving the data or manipulating it in some way to hide the vessel's identity. However, blocking or tampering with AIS data is illegal. SOLAS V/34-1 states: *"The owner, the charterer, the company operating the ship as defined in Regulation IX/1, or any other person shall not prevent or restrict the master of the ship from taking or executing any decision which, in the master's professional judgement, is necessary for safety of life at sea and protection of the marine environment"*. So, if a reasonably prudent master considers AIS necessary for the safety of the vessel (which they should of course do), blocking or tampering with the signal is likely out of the question.

It might be possible to enter into an agreement with each of the individual companies making AIS data available to the public not to publish the AIS data about a particular yacht or yachts. Whilst in theory this would be possible, the service providers will expect something in return. Further, given the plethora of sites publishing AIS data it will be difficult to reach agreement with all and, even if you do, more may emerge.

TOM WALTERS
Partner, London
T +44 (0)20 7264 8285
E tom.walters@hfw.com

MARK THOMPSON
Senior Master Mariner, London
T +44 (0)20 7264 8528
E mark.thompson@hfw.com

France steps up its defence of posidonia meadows and its environment

As previously reported in this publication, since October 2020, France has banned the anchoring of Yachts over 24 meters in certain areas, mainly on the Côte d'Azur and Corsica, in order to protect the vital posidonia grass meadows. The Code des Transports sets out severe penalties for those who breach these anchorage regulations. Such penalties range from a temporary or permanent ban from sailing from French ports and in French territorial waters up to a year's imprisonment and a EUR 150,000 fine.

In an unprecedented move, on 20 October 2023, the Maritime Court of Marseille handed down the first judgment regarding breaches of these regulations. In doing so, it convicted the captain of a 26-meter yacht for having, on three occasions in 2021 and 2022, anchored his yacht in prohibited areas offshore Cannes and Saint-Tropez. The captain was fined EUR 20,000 and banned from sailing in French territorial waters for one year.

As was emphasized by the various environmental associations which joined the proceedings as plaintiffs, the permanent or temporary ban on sailing from French ports and in French territorial waters is considered a particularly effective sanction when it comes to deterring other yacht captains from committing the same offences.

The Court also ruled that the captain's actions had caused "significant damage to ecosystems" and ordered him to pay compensation for the "ecological damage" caused by these actions. To estimate the economic value of the damage, the Maritime Court requested the assistance of the Environmental Unit of the Court of Marseille. This point will be debated at a further hearing set for 26 January 2024.

The regeneration of posidonia meadows is a slow process, which requires significant human intervention (such as replanting by the Water Agency, a French public body currently engaged in a project to protect posidonia meadows). One of the environmental associations involved has estimated the damage caused by the captain's actions to amount to nearly EUR 60,000.

Although damage to the environment is a fairly new concept in French law, since it was introduced to the French Civil Code only in 2016, French judges now regularly apply it and are willing to admit claims made by local communities and environmental associations in respect of it. In a previous decision of 6 March 2020, concerning illegal fishing in the National Park of the Calanques (a protected area), the Criminal Court of Marseilles ordered the defendants to pay EUR 350,000 in damages, to be allocated in its entirety to repairing the damage caused by their actions to the National Park's ecosystem.

The judgment by the Maritime Court of Marseille is likely to be the first in a long series of such judgments and it is to be expected that sanctions will become harsher as time goes by and the consequences of illegally anchoring in posidonia meadows and the costs of their restoration becomes clearer. Yacht owners and their captains should take seriously the threat this judgment posses to them.

HÉLÈNE DE FERRIÈRES
Senior associate, Paris
T +33 (0)1 44 94 31 41
E helene.deferrieres@hfw.com

Cyber Security, Take it Seriously!

Cyber-attacks continue to dominate the news, with recent political tensions and war highlighting society's reliance on, and the vulnerability of, computers and the connectivity which they provide. Whilst some of the most serious attacks last year involved the loss of very significant sums of money by their victims[3], it is becoming increasingly clear that cyber-attacks can, in addition to causing financial and reputational damage, also potentially cause a threat to life and limb, property and the environment[4].

In January 2023, about 1,000 ships were affected by a ransomware attack when the international classification society, DNV, was attacked and forced to shut down its IT servers and ShipManager System. DNV has since published its report on the attack entitled *"Maritime Cyber Priority 2023,"* which includes results from a survey of 801 maritime professionals covering the perceived threats, preparedness and challenges related to cyber security[5]. More than 60% of those surveyed expect cyber-attacks to cause ship collisions and groundings within the next few years, and 76% of those surveyed believe a cyber incident is likely to force the closure of a strategic waterway.

The yachting industry must adopt a robust approach to cyber-security. Such an approach should be built in from the very beginning of the design process and maintained throughout a yacht's life. Cyber-attacks on yachts typically threaten privacy and reputation,and focus on the theft of financial and personal data as well as financial crime. Typically, they are launched through ransomware or malware attacks on the yacht itself or the devices of its guests and/or crew.

However, they can go further. Once a system has been attacked and breached, threat actors can go on to do anything from stealing personal data to gaining and maintaining full access to a device, potentially jeopardising the safety of both the individual and the operational integrity of the yacht.

We have previously reported on the update to the International Safety Management Code (the **ISM**) requiring all commercially operated vessels to address cyber security in their Safety Management System (the **SMS**) in accordance with MSC-FAL.1-Circ 3 and IMO Resolution MSC.428(98). The resolution also encouraged Flag States to ensure that cyber risks are appropriately addressed in SMS no later than the first annual verification of the company's Document of Compliance (the **DOC**) after 1 January 2021.

In response to this development, the International Association of Classification Societies (**IACS**) introduced new Unified Requirements (**URs**) on cyber safety with the aim of developing a vessel's resilience and helping ship owners strengthen their cyber security arrangements[6].

URs E26 and E27 respectively deal with the cyber resilience of ships and the cyber resilience of onboard systems and equipment. They consolidate the requirements for cyber safety onboard ships and will be implemented by the eleven IACS member societies on ships contracted for construction on or after the 1 July 2024[7]. These URs build on IMO Resolution MSC.429(98)/Rev.1 and the guidance in MSC-FAL.1/Circ.3.

The URs have been categorised as "mandatory" and "non-mandatory" depending on vessel type and size. E26 and E27 will apply to privately registered passenger yachts carrying

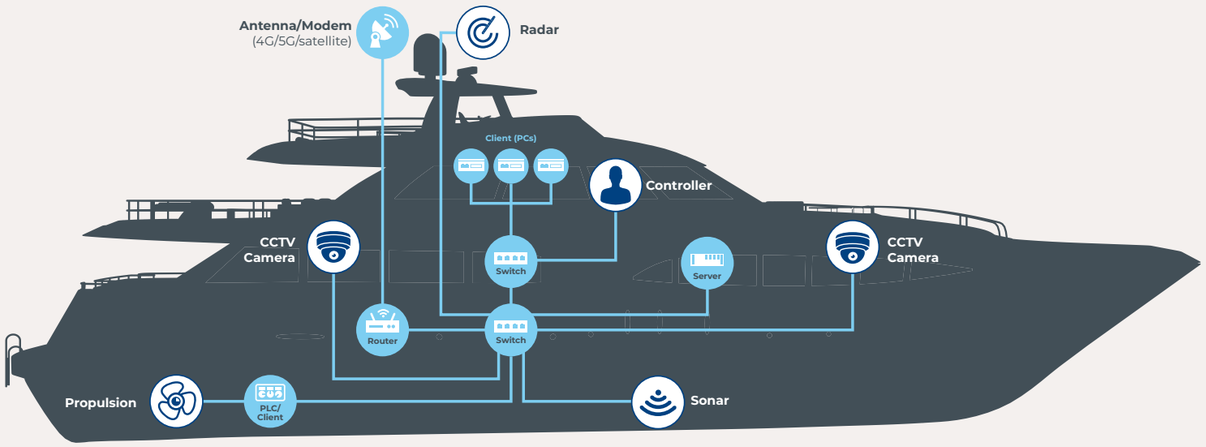
3 Crypto were hacked in January 2022 resulting in the unauthorised withdrawal of bitcoin and Ether worth around $35 million. Axie Infinity, an online video game, were allegedly attacked by North Korean hackers from the Lazarus Group who stole an undisclosed sum. The U.S. government recovered about $30 million of the stolen funds. Medibank were attacked in October 2022 and the attackers demanded a ransom payment of $9.7 million not to publish stolen data. Medibank refused to pay and the hackers then threatened to release data each day the ransom remained unpaid. The attack was estimated to cost Medibank $25 to $35 million.

4 https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/

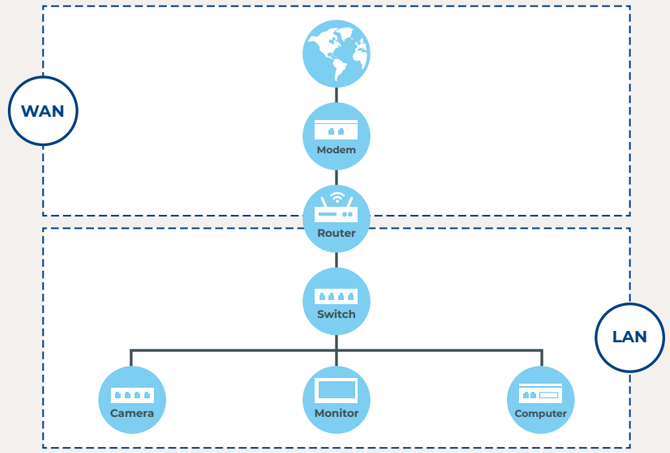
5 https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html

6 https://insurancemarinenews.com/insurance-marine-news/iacs-adopts-new-requirements-on-cyber-safety/

7 https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release



Above: A simplified computer network, including a selection of peripherals (marked in white)



A simplified Local Area Network (LAN) which incorporates some of the systems and equipment opposite

more than 12 passengers and commercial yachts[8].

It is important to underline that the URs introduce new standards for the cyber resilience of not only the systems and equipment onboard but for the vessel as a whole. They will naturally increase the responsibilities of shipyards and manufacturers, who will now be required to check the integrity of a vessel's systems before they are installed. This new layer of checks may prove time-consuming and could ultimately delay newbuild projects if not properly considered in the production schedule. Many of the checks themselves will be highly technical in nature, and thus require a certain level of expertise from the personnel engaged in the process[9] and it will be for the classification society overseeing the construction to ensure the vendor systems comply with the URs[10] and duly certify themselves. Whether the yacht building industry has sufficient suitably qualified personnel to carry out this work remains to be seen.

After 1 July 2024, the owners and managers of any yacht to which the URs apply must ensure that the yacht's ISM deals with the mitigation of cyber risks and that they have established safeguards against all risks to ships, personnel, and the environment. The new URs will complement existing UR E22, which relates to the onboard use and application of computer-based systems. Whilst the new URs will not apply to all yachts, it would be prudent for all yachts to take them seriously and do what they can to comply.

UR E26: The vessel's cyber-resilience as a collective entity[11]

UR E26 is to be uniformly implemented by IACS members and its purpose is to make vessels cyber resilient[12]. The intention is for this to be achieved through "the secure integration of both Operational Technology (**OT**) and Information Technology (**IT**) equipment into the vessel's network during the design, construction, commissioning, and operational life of the ship"[13].

The following stakeholders will be required to comply with the requirements:

1. Shipowner Company
2. Ship Designers and Shipyards
3. System Integrators
4. Suppliers
5. Classification Societies

Further, UR E26 covers the five functional elements summarised in the table attached at the end of this article[14]. Each of these five elements introduces its own requirements. These are highly technical in nature and are to be addressed by the suppliers and shipyards. The appendix to UR E27 sets out a useful summary of the relevant phases, actions and documents involved. There are identified as:

1. Design
2. Construction
3. Commissioning
4. Operation
5. Survey

The "Shipowner Company" is engaged only in the Operation and Survey phases. Interestingly, the obligations of the shipowner are merely to "maintain" or "make available.", as per the Appendix's wording. This means that shipowners have to make sure documents are kept up to date and made available if needed. By contrast, the role of the classification society, supplier, shipyard and system integrator in the process is considerably more demanding.

That being said, owners should still stay alert and are encouraged to actively participate in the process, especially when it comes to agreeing vessel specifications. During negotiations and other relevant arrangements with shipyards and suppliers, owners should ensure the requirements of UR E26 are met. This is not only to ensure compliance with UR E26 but also to mitigate the risk of the classification society refusing to sign-off a vessel. Further, after a newbuilt vessel is delivered, owners will have to make sure that software and systems onboard as well as incident response plans are suitably maintained.

UR E27: cyber-resilience of onboard systems and equipment

This UR establishes another set of minimum requirements which are applicable to Computer Based Systems[15] (**CBS**) referred to in UR E26.

Pursuant to UR E27, "a System can consist of group of hardware and software enabling safe, secure and reliable operation of a process"[16]. UR E27 goes on to specify the security capabilities necessary for compliance with this UR, which are required for all CBSs.

The documentation relevant to these systems shall be submitted to the classification society, for its review and approval.

"Equipment" could refer to:

- Network devices (i.e. routers, managed switches) – e.g. a modem which connects the vessel to the internet via a 4G, 5G or satellite connection. A router allows the local network to share a single internet connection and creates a subnet by assigning IP addresses or names to all the other devices on the network. A switch physically directs data to devises on the network.
- Security devices (i.e. firewall, Intrusion Prevention System).
- Computers (i.e. workstation, servers) e.g. monitors from which you can navigate the yacht or control the vessel.
- Automation devices (i.e. Programmable Logic Controllers).
- Virtual machine cloud-hosted[17].

Legal and practical considerations

Installing and maintaining a robust cyber security system covering all of the systems and equipment onboard, as well as the vessel as a whole, is essential. Any vessel contracted for construction after the 1 July 2024 must be fit from a cyber-security perspective if it is to be signed off by the relevant classification society.

Stakeholders should consider the following:

- If Class approval is not obtained, this could trigger a domino effect with serious consequences. For instance, the vessel's seaworthiness could come into question. This could not just create problems from an insurance perspective, with insurers being reluctant to provide cover, but also lead to claims being made against owners. These could be brought by, among others, charterers or guests or insurers.
- Insufficient cyber-security measures could pose a threat to the availability of insurance cover. Potential exposure of Hull & Machinery and Protection & Indemnity insurers to liability in the event of an incident could mean that there would be no cover or security provided. Inadequate cyber-security systems onboard could also lead insurers to demand that a vessel

8 E27 is 'non-mandatory' for e) passenger yachts (passengers not more than 12) and f) pleasure yachts not engaged in trade - https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103853/UR-E27-Rev.1-Sep-2023-CLN.pdf

9 Ibid.

10 https://www.dnv.com/expert-story/maritime-impact/Yards-and-vendors-must-act-promptly-to-comply-with-upcoming-IACS-cyber-security-requirements.html

11 https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/

12 https://www.american-club.com/files/files/ur-e26-new-apr-2022.pdf

13 https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/

14 https://www.american-club.com/files/files/ur-e26-new-apr-2022.pdf

15 https://www.classnk.com/hp/pdf/info_service/iacs_ur_and_ui/ur_e27_rev.1_sep_2023_cln.pdf which defines a CBS as "A programmable electronic device, or interoperable set of programmable electronic devices, organized to achieve one or more specified purposes such as collection, processing, maintenance, use, sharing, dissemination, or disposition of information. CBS on-board include IT and OT systems. A CBS may be a combination of subsystems connected via network. On-board CBS may be connected directly or via public means of communications (e.g. Internet) to ashore CBSs, other vessels' CBS and/or other facilities".

16 https://www.american-club.com/files/files/ur-e27-new-apr-2022.pdf

17 Ibid.

is brought up to the specifications necessary for cover to be available, after construction is completed.

- More sophisticated IT systems onboard could also impact policy wordings. The latter could be updated, especially given the requirements introduced by the URs are "minimum" and therefore insurance providers could demand higher thresholds to be met.
- If cyber risks are not appropriately addressed in the respective safety management system and/or the URs are not in generally complied with, flag states may also refuse to issue compliance documents to vessels.
- The extra layers of work required in the process of cyber-proofing a vessel could prolong the construction and design processes and increase costs.
- While the burden of cyber-proofing a vessel during construction is placed more on suppliers and shipyards, prospective owners are encouraged to oversee the process, carry out checks and ensure URs are complied with.
- Vessel owners should ensure the anonymity of their guests is well preserved. Any data breaches resulting from network systems onboard being compromised could cause serious concerns and lead to claims being brought forward.

TOM WALTERS
Partner, London
T +44 (0)207264 8285
E tom.walters@hfw.com

MAIRA LOUKAKI
Associate, London
T +44 (0)20 7264 8784
E maira.loukaki@hfw.com

No.	Functional element	Element sub-goal	Requirement	Requirement details
1	**Identify**	Develop an organizational understanding to manage cybersecurity risk to onboard systems, people, assets, data, and capabilities.	Inventory of Computer Based Systems (CBSs) and networks onboard	CBSs' inventory of hardware and software to be available and properly updated for the entire life of the vessel.
2	**Protect**	Develop and implement appropriate safeguards to protect the ship against cyber incidents and maximize continuity of shipping operations.	a. CBSs to be grouped into security zones	Security zones to be segmented as required.
			b. Network protection safeguards	Data flow safeguards to be implemented.
			c. Antivirus, antimalware, antispam and other protections from malicious code	Software or physical safeguards to be used for anti-virus and anti-malware purposes.
			d. Access control	Relevant CBSs and networks and the information included therein to be accessible by authorised individuals, processes and devices.
			e. Wireless communication	Suitable cryptographic mechanisms to be applied to enhance integrity and confidentiality.
			f. Remote access control and communication with untrusted networks	Clear guidelines and manuals to be produced for IT and OT systems involved.
			g. Use of mobile and portable devices	Mobile and portable devices to be listed in inventory list, together with any maintenance-related information.
3	**Detect**	Develop and implement appropriate measures to detect and identify the occurrence of a cyber incident onboard.	a. Network operation monitoring	Adequate measures to monitor networks and, if required, intrusion detection systems to be implemented.
			b. Diagnostic functions of CBS and networks	Relevant CBSs and networks to be able to check performance and functionality of security functions to verify intended operations and signal detected anomalies
4	**Respond**	Develop and implement appropriate measures and activities to take action regarding a detected cyber incident onboard.	a. Incident response plan	Plan specifying how to respond to cyber incidents, including a comprehensive set of instructions and certain types of information for the shipowner
			b. Local, independent and/or manual operation	Any CBS required for local backup control to be independent from other CBSs
			c. Network isolation	Network segments to be capable of being isolated (manually or automatically) and relevant instructions to that effect shall be available.
			d. Fallback to a minimal risk condition	In the case of a cyber incident, affected system or network to fall back to a minimal risk state in which a reasonably safe condition can be attained.
5	**Recover**	Develop and implement appropriate measures and activities to restore any capabilities or services necessary for shipping operations that were impaired due to a cyber incident.	a. Recovery plan	Recovery plan to be comprehensible and entail essential instructions and procedures to be followed following system failure.
			b. Backup and restore capability	Ship to regain navigational and operational capabilities in a timely, complete and safe manner.
			c. Controlled shutdown, reset, roll-back and restart	Relevant CBS and networks to be in a position to perform these functions and appropriate documentation to that effect to be available onboard.

COMPREHENSIVELY YACHTS

The HFW yacht team has been an integral part of the yacht industry for over 30 years and has a physical presence in many of the major yachting jurisdictions. The enduring relationships developed with the owners, builders, designers, financiers, insurers, brokers and managers of yachts, our in-depth knowledge of the yacht industry and our international reach ensure we are pre-eminent in the field. For more information on HFW's yacht team and the services we offer, please see **www.hfwyachts.com**

© 2023 Holman Fenwick Willan LLP. All rights reserved. Ref:005553

Images used with kind permission of Breed Media Creative Limited.

Whilst 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. Holman Fenwick Willan LLP is the Data Controller for any data that it holds about you. To correct your personal details or change your mailing preferences please email hfwenquiries@hfw.com

Americas | Europe | Middle East | Asia Pacific