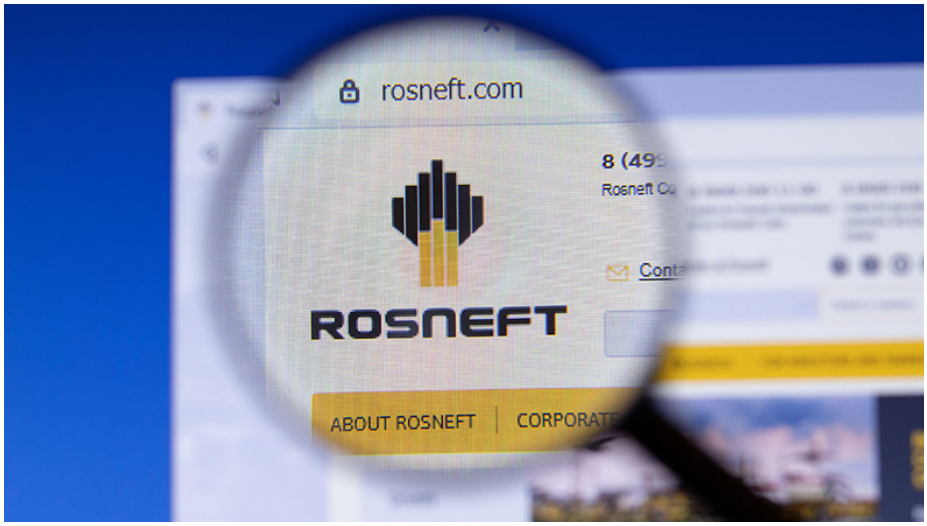
Lloyd's List
Maritime intelligence | informa

Daily Briefing
Leading maritime commerce since 1734

Credit chaos and emergency due diligence as shipping continues to shun Russia



CRISIS MEETINGS IN boardrooms across the maritime sector continue to see trades exposed to Russia put on hold or abandoned completely amid growing concerns over sanctions and potential risks associated with Russian-linked counterparties.

Compliance departments in shipping companies last week started removing Russian entities from approved lists, while credit lines were withdrawn and many companies issued blanket internal notices to halt Russian-related transactions.

"There is a huge amount of potential trade out there that does not touch sanctions, but the trades cannot be facilitated because the banks are not there to execute the trade," one chief executive told Lloyd's List following a three-hour board meeting that saw his bunker supply company cease trading with all Russian counterparties and halt supply to Russian ports.

Several banks have started refusing to issue letters of credit to cover Russian crude, however following announcements from several governments pledging to block certain Russian banks' access to the Swift international payment system over the weekend, the reluctance to cover credit to any Russian counterparty has escalated across the shipping sectors.

For markets like bunkers that rely heavily on credit and post-payment, the withdrawal from Russia has been swift.

For companies with Russian exposure that cannot be abandoned so easily, there has been a rush to seek legal guidance on managing risk.

"There has been an elevated level of enquiry from clients looking to assess their Russian risk exposure," said Daniel Martin, a partner and sanctions expert at law firm HFW. "We are fielding calls from clients across the sector looking to understand their exposure and how to mitigate this in light of the changing legal landscape.

"Clients are in a hugely challenging position because of the legal complexity of the measures, the very significant amount of ongoing trade with Russia, and the extent to which sanctions measures are being announced by politicians prior to the legal instruments being published."

Other law firms have issued blanket bans on partners talking publicly about Russia, such is the political sensitivity from clients exposed to the turmoil.

Inside banks, officials and legal teams are understood to be "scrambling to decide what it means", with insiders warning that policy is unlikely to catch up with political rhetoric until treasury departments can issue guidelines.

Those companies prepared to make statements are largely sticking to the line that it is business as usual until such time as sanctions measures directly target shipping entities.

However, off the record, multiple senior shipping company insiders are characterising the current situation as "chaotic" and "very dynamic".

Lloyd's List understands that several major bunker suppliers have now ceased trading with Russian counterparties completely and most stopped supplying Russian and Ukrainian ports more than a week ago.

"Rather than spending time and potentially thousands of dollars in legal fees proving due diligence in the event that authorities question trades, we are sitting it out and waiting to see how things pan out," said one bunker supplier executive. "If we feel that there is a reasonable way to restart, we may consider but at this point of time, we are not touching Russian counterparties — it's too risky."

Oil majors BP and Norway's Equinor have announced that they would be exiting investments in Russia. BP said it would exit its 19.75% shareholding in Rosneft that it has held since 2013.

Elsewhere, companies with an existing client base of Russian interests have been quietly considering exposure and performing urgent due diligence checks on Russian beneficial ownership links.

For classification societies with Russian owners and vessels, the current line continues to be that they are monitoring political developments closely, but so far no changes have been made.

"We are keeping abreast of the widening sanctions requirements as they are enacted and anticipate we will be further updating our compliance requirements in this regard," a Lloyd's Register spokesperson said. "We are keeping in close touch with external advisors to help ensure LR's compliance programme is updated as required.

"In recent years, LR has had very limited involvement with vessels owned or managed by Russian interests."

A spokesman for DNV said: "We are currently reviewing all ongoing contracts and operations with Russian entities. DNV is committed to complying with all relevant international sanctions."

Remi Eriksen, DNV group president and chief executive officer, said: "We are deeply disturbed by the invasion of Ukraine, which is inflicting terrible harm to the citizens of Ukraine and threatening peace across the region. Our top priority is the safety of our people, and we are working to ensure our employees have the support they need."

UK bans port access to all Russian-linked vessels

THE UK has told its ports to block any Russian-linked vessels.

"The maritime sector is fundamental to international trade and we must play our part in restricting Russia's economic interests and holding the Russian government to account," Transport Secretary Grant Shapps said in a letter to all UK ports.

Further detailed sanctions against Russian shipping were being drawn up following Russia's invasion of Ukraine, he added.

Describing the military operation as an "unprovoked, premeditated attack against a sovereign democratic state," Mr Shapps said the UK government "does not consider it appropriate for Russian vessels to continue to enter UK ports."

He advised ports to refuse any ship they believe to be owned, controlled, chartered or operated by any person connected with Russia or a sanctioned person or flagged or registered in Russia.

While the letter said support would be given, it did not detail how ports would impose the guidance or identify Russian links.

There are currently 16 Russian flagged vessels in UK waters and four vessels owned by sanctioned Russian operator Sovcomflot, according to latest Lloyd's List Intelligence vessel-tracking data.

"The maritime sector is fundamental to international trade and we must play our part in restricting Russia's economic interests and holding the Russian government to account," the letter explained, adding that legislation would follow.

The UK move follows protests in the Orkney Islands over Sovcomflot's 106,000 dwt aframax tanker *NS Challenger* (IMO: 9299680) arriving at the Flotta Terminal.

The US has imposed financial restrictions on Sovcomflot, Russia's largest shipping company, as part of the broader sanction moves to hold Moscow accountable for its military incursion into Ukraine.

The letter issued by Mr Shapps indicated that the move to ban Russian vessels was part of a broader package of further sanctions, the details of which will be released shortly.

Britain has already banned Russia's Aeroflot airline from flying to the UK.

Tanker rates at 'high and volatile' levels on Ukraine impact

TANKER rates in the short term are likely to remain elevated and volatile, especially in the Baltic and Black Sea regions as the Ukraine situation continues.

Poten & Partners made this forecast as spot rates, especially those for aframaxes and suezmaxes, have surged over the past few days as tension between Russia and Ukraine has escalated.

From February 24 to February 25, the suezmax time charter equivalent weighted average increased nearly sixfold to $67,027 per day, according to data from the Baltic Exchange. The average aframax rate increased by 596% from the start of the week to Friday, surpassing $40,000 per day. Very large crude carriers rates saw a small bump but still sit in the negatives.

In a series of sanction moves against Moscow, the US and its western allies have unveiled by far the most punitive measures by blocking its central bank and removing some of its banks from the Swift financial messaging system, which allows the secure and efficient transfer of money across borders.

"None of these sanctions directly targets the Russian oil and gas industry, but the oil and tanker markets have been significantly affected nevertheless," said Poten.

Freight rates spiked on various export routes from the Baltic and Black Sea, partly because owners facing security risks and compliance uncertainties are reluctant to charter vessels to buyers of Russian crude.

Poten said at least three commercial vessels, comprising two bulk carriers and a bunker tanker, have claimed to have been hit in the Black Sea since the Russia-Ukraine conflict started.

"Until hostilities are reduced, many shipowners will likely avoid this area, through which Russia exported on average 1.7m barrels per day of crude oil in 2021."

Meanwhile, Urals crude is being sold at a discounted price as traders and bankers are shunning Russia-related transactions.

"Potential buyers are also having difficulty obtaining letters of credit from Western banks to finance the purchase," said Poten.

Gibson Shipbrokers also noted that fewer companies are willing to trade and transport Russian commodities.

"Many large companies, particularly those which are public, will not want to be seen supporting the

Russian economy," it said the latest weekly report.

The combination of freight rate premium and the pump price discount in the region, however, will still encourage audacious owners and charterers to continue the trade, with a potential shift of cargo flows to Asian destinations, particularly China.

The bigger question is whether the European Union, the largest buyer of Russian crude, can find enough supplies from alternative sources, such as the US and the Middle East.

If the EU can do this, it will bode well for tankers as the tonne-mile demand will increase significantly.

The prospects remain unclear, at least in the short term.

"The oil market was already tight and reduced export flows from Russia cannot easily be compensated for by other exporters," said Poten.

Braemar ACM said the 23-nation Organisation of the Petroleum Exporting Countries-plus alliance appears unlikely to release more crude into the market until it is convinced that supply shortage is real, while the US shale exporters are responding more slowly than usual to the higher oil prices.

But the brokerage predicts that enquiries will pick up sharply for West African and Mediterranean crudes.

Elsewhere, "North Sea crudes are an obvious substitute for Urals into Europe," it said. "Iraqi Basrah crude could move in greater volume to Europe, but current steep backwardation in the oil price makes such long-haul voyages less attractive."

Both Poten and Gibson expect freight rates to remain high and volatile over the next few weeks, pending the development of the Ukraine situation.

The market fundamentals, which remain weak for tanker shipping, mean rates could fall back if the situation becomes clearer and the tension eases off, said Poten.

But a further escalation of sanctions in relation to blocking Russian exports would result in "more dislocations and inefficiencies in the market."

These inefficiencies may be in the form of long-haul movement replacing current short-term haul trades, probably resulting in sustained higher tanker rates, Poten said.

Gibson argued that if Russia's crude exports are hit by stricter sanctions, increased longer-haul imports into Europe will support tankers' tonne-mile demand if there is sufficient volume to compensate the losses. "Uncertain times ahead," it said.

Shipowners and charterers have largely been holding back on engaging in any new-period business, with most waiting to see the outcome, according to Braemar.

"Some owners have been indicating high time charter rate ideas today but charterers have not yet been persuaded by current events to pursue further," it said.

Maersk considers suspending shipments in Russia as sanctions escalate

THE growing threat of sanctions against Russian entities is adding yet more potential disruption to containerised supply chains, although at this stage their impact remains uncertain.

Maersk said it was closely monitoring and preparing to comply with "the ever-evolving sanctions and restrictions imposed against Russia".

"Our preparations include a possible suspension of Maersk bookings to and from Russia on ocean and inland," it told customers in an advisory. "We are at the same time keeping a close eye on developments and assessing the best options for our customers and their cargo."

Sea-Intelligence chief executive Alan Murphy said that while it did not appear to have a major impact specifically on container shipping, there was enough uncertainty that carriers were choosing different risk profiles.

"Most still take bookings to Russia, but caution that conditions may change at short notice, whereas Hapag-Lloyd, for example, has temporarily suspended bookings to Russia."

The wider implications of any sanctioning of Russian use of the Swift banking network remained unknown, but there was a risk of an impact to Russian shippers and consignees if their

banks were unable to use the network, he added.

"Given that the war in Ukraine shows no signs of abating, it is an open question whether even more sanctions will happen," he said. "Presently, it is not possible to predict even a few days into the future, and all bets are off in relation to the viability of Russian cargo and routings."

Maersk said it would do what it could to deliver cargo already on the water to its intended destination.

"We have a sharp focus on safeguarding reefer containers and keeping cold chain operations as stable as possible, as the commodities include important goods such as groceries and pharmaceuticals," Maersk said.

"We are doing everything possible to prevent risk to the above cargo and in turn risk to the end-users in need of these commodities. It's also worth noting that air space is also gradually being restricted and our air services will be impacted."

Maersk has also started offering a set of relief measures for customers with cargo destined to or from Ukraine.

These include free change of destination services and no cancellation fees for cargoes to Ukraine.

But to prevent further congestion at key ports, it is moving Ukraine cargo to ports with less cargo density and which have sufficient reefer plugs for perishable commodities.

Meanwhile, the European Shippers' Council said the military operation in Ukraine would "certainly influence international trade and logistics".

"The sanctions imposed by the international community on Russia, and possibly on Belarus, will also be noticeable to European entrepreneurs," it said. "It is important for entrepreneurs in international trade and logistics to be informed as well as possible about the consequences of the raid and sanctions to be able to properly assess the impact on their own business operations."

It warned of stricter controls at borders between Russia and Ukraine and a number of EU member states, and said the China-EU railway, that runs via Russia and Belarus to Poland could be affected.

"It is still unknown whether this railroad line is still functioning properly," the ESC said. "Russia transports a lot of military equipment to Belarus via this railroad."

The impact of sanctions issued by the European Commission that come into effect on Friday, is still unclear, but these will affect transport, energy and financial sectors in Russia.

"The raid and sanctions affect the coverage of various insurance policies, such as credit insurance and transport insurance," the ESC said. "The impact on international trade will vary by sector and depends on how the conflict develops."

Analysts at Linerlytica, however, were more positive about the impact of sanctions on Russia.

"The Russia-Ukraine conflict will not have a material impact on global container trade volumes, as the total Ukrainian container throughput of 1m teu in 2021 accounts for just 0.1% of global container volumes," Linerlytica said.

"Even if economic sanctions affect container volumes in Russia, the total impact on global container trade volumes will be just 0.6%. However, not all of the Russian container volumes would be affected as the growing Russian Far East container trade through the ports of Vladivostok and Vostochnyy is expected to continue to thrive."

Bulker owners try to avoid Black Sea amid war escalation

BULKER owners are trying to avoid the Black Sea area as the conflict rages between Russia and Ukraine.

Some are also avoiding doing business with Russian companies in light of sanctions.

Denmark's Norden said it was "saddened" to witness Russia's military incursion into Ukraine, adding that its thoughts were with the people in the region.

"We have adjusted our business to align with the newest sanctions and have furthermore decided that as of today, Norden will not take in any new Russian business nor call at Russian ports. We will continue to fulfil our existing contracts, as we are legally obliged to do."

Another Danish company, Lauritzen Bulkers, said it had decided to stop all trading in and out of Russian and Ukraine ports.

It also stopped entering new deals with Russian companies, and this "will be maintained for the time being".

"We are slowly getting out of existing deals, but still have funds outstanding with Russian accounts from deals done before the crisis," it said. "This is of course making our trading difficult, but more importantly, a terrible humanitarian crisis that is 100% man-made and completely unacceptable."

Norway's Golden Ocean said it had only one vessel loading in the southern part of the Black Sea, and all going well, will complete loading later in the week. "At this point, there have been no disruptions or threats to the vessel or its crew."

"Our exposure to the Black Sea is mainly spot-oriented, but for the time being, we are avoiding the area and are finding alternative employment," it said, adding that although it has not been necessary to re-route vessels or cancel contracts, it was monitoring developments "around the clock".

Germany's Oldendorff said it had one bulker at Odessa port at the start of the war, which safely sailed away. It has had to make other plans for ships planning to go to the Black Sea.

"Most owners and operators will want to stay well clear," said a spokesman. "Insurance will make trade to that area prohibiting."

A US-based owner of smaller-size bulk carriers said it will avoid the region, which only represents a fraction of its business, at about 3% of traded volumes per year.

Meanwhile, there were reports that some bulkers were hit by shelling in the past week, prompting flag states to issue advisories strongly encouraging all vessels to avoid transit in Ukrainian and Russian waters in the Black Sea and Sea of Azov.

Flag states have also advised vessels in the Black Sea to increase security measures and conduct voyage-specific risk assessments and "exercise extreme caution when operating in these areas".

While spot capesize rates took a knock at the close of trading on February 28, handysizes showed the biggest gains.

Average capesize time-charter slipped 12.5% to $13,414 per day from a week ago and 26% from February 23, according to the Baltic Exchange.

While panamaxes dropped 3.7% to $23,389 from a week ago, rates are in fact 6.5% higher than mid-week last week.

Supramaxes gained 3.7% to $26,711, while handysize rates were up 7.6% from a week ago, Baltic Exchange data shows.

ANALYSIS:

Chief executives are first line in solid cyber-security defence

IN its cyber-security guidelines for ports and port facilities, the International Association of Ports and Harbors describes cyber risk as the "unavoidable handmaiden" to digitalisation.

The number of cyber attacks on ports, shipping and the wider logistics supply chain cannot be accurately quantified. However, it is clear that the deeper the maritime industry gets into digitalisation, the more vulnerable it becomes.

Protecting the industry from hackers is not rocket science. Guidelines on cyber security have been issued from all the industry associations and are aligned with the International Maritime Organization's stipulation that cyber risks must be appropriately addressed in existing safety management systems no later than the first annual verification of the company's Document of Compliance after January 1, 2021.

The most critical first step towards protection is for the C-suite to take responsibility for cyber risk. Security is a collective remit that is not solely limited to the IT department.

"Senior management should embed a culture of cyber-risk management into all levels and departments of an organisation," states the latest version of industry guidelines led by BIMCO.

It adds that senior managers should ensure a "holistic and flexible" cyber-risk governance regime, which is in continuous operation and constantly evaluated through effective feedback mechanisms.

The significance of this first step is often overlooked in the rush for technical solutions.

"Being able to assure yourself, your clients and your supply chain of the integrity of the data flowing through and across your systems is becoming part of the fabric," Inmarsat Maritime president Ben Palmer told Lloyd's List.

"While it's an obvious truism, I'm not sure everyone has fully absorbed what it means in practice. Managing response plans and managing the reality of the situation will be 'de rigeur', as well as trying to ensure against it."

Mr Palmer, who brings experience to maritime from the defence and aviation sectors, said cyber security tends to be presented as a technological problem, although the human dimension is just as important.

IAPH agrees. Its guidelines recommend that C-suite executives should take the lead in allocating resources to deal with cyber security, actively managing governance and building an organisational culture to support cyber-security operations, and developing leadership strategies for driving cyber resilience, including the creation of a cyber-security workforce.

The ports' association focuses on developing a business case for the executive team to determine a reasonable level of investment in cyber-risk management. Its conclusion should be taken on board by ship operators and managers alike.

Port managers weigh up whether a proposed level of investment is enough and whether the return on investment justifies the spending.

They argue that trade-offs are constantly being made in a competitive world; that cyber risk is insurmountable — a belief that prohibits proactive investment in key resources; that cyber risk is difficult to quantify and depends on subjective analysis; and that the hardest thing to change is human behaviour.

Such justifications reveal a common perception plaguing executive suites: that investment in cyber security is often considered a cost centre, rather than an enabler of port operations.

Once the senior management is on board, the second step is to manage risk itself.

There are several elements to this, beginning by identifying the external and internal nature of threats, identifying which systems are liable to attack, and assessing exposure to risk.

Once vulnerability is understood, the necessary protections can be built. Protection and detection measures can be agreed, response plans established, and analysis made following a cyber incident.

The ship-to-shore interface, where cyber security for ships and cyber security for ports overlap, can present one of the most vulnerable nodes of the supply chain network.

"Think about the interfaces," Mr Palmer urges. "People tend to think about the standalone thing they own, but it's the interfaces where things go wrong, where there are leaks. That makes it an enterprise problem as opposed to individual actors securing their bit of it."

All cyber-security guidance stresses the importance of the human element alongside the technology. One document states: "It cannot be stressed enough how important it is to raise the awareness and vigilance of crews regarding cyber security.

"Crew training may look like a simple and inexpensive measure to implement, yet it represents the smartest investment in this area."

Given the range of threats and attacks, from phishing — the most common form of social engineering attack by individual opportunists — to state-backed cyber warfare, it is important to be aware of an attacker's level of competence.

Some attacks are unintentional, perhaps introduced by a USB stick; the 'standard' attacker will use hacking tools and techniques to gain access to a system; and the 'criminal' attacker will invest time and money to gather intelligence about the company, fleet or vessel.

The best line of defence begins when senior management takes responsibility at an enterprise level, builds a culture of security, and trains sea and shore staff in correct procedures. Cyber-security technology works best when the human element is in place.

Cyber-risk insurance: Not as easy as you would think

THE past five years have seen a spate of cyber attacks on big names in the maritime industries, with victims including Maersk, Clarksons, CMA CGM, HMM, MSC and even the International Maritime Organization itself.

Companies have found themselves substantially out of pocket; the hit to Big Blue in 2017 may have been anything up to $300m.

There has yet to be a major casualty at sea that can directly be attributed to cyber events. However, most experts consider that only a matter of time.

In principle, any shore- or ship-based electronic, navigation or computer system is vulnerable to the unwanted attentions of hackers, be they hobbyists, criminals or terrorists.

There need not even be malevolence at work. A lost laptop or an unencrypted email can result in a serious breach of security.

Certainly such exposure is becoming a concern of major charterers, who are increasingly asking shipowners to evidence the level and scope of their cyber-assessment processes and the control, mitigation and recovery plans they have in place.

The issue should not be beyond the ingenuity of the marine insurance sector to resolve, and bespoke products are already available. Yet the process has not been as straightforward as it should be.

To begin with, underwriters cannot agree among themselves as to whether cyber is best written in a marine book, a political risks book or a bespoke cyber book. Everyone seems to have a different view.

Then there is the relatively new nature of cyber attacks, which did not exist until recent times. Without historic data, it is difficult for underwriters to build actuarial models that quantify and price the risk.

Indeed, there has been a natural tendency on the part of insurers to overprice cyber — which, unsurprisingly, has inhibited uptake.

The Catch-22 is that the embarrassment factor has meant some companies have not publicly divulged cyber attacks. That makes it difficult for the underwriters to obtain data as a basis for quotes in the first place.

James Cooper, managing director of one the few marine cyber specialists, Astaara, describes this as being a key problem when the company was set up.

“As a good, prudently regulated business, we had to understand what we were pricing for and why we were pricing for what we were doing. There was not enough data around,” he said.

Fortunately, surrogate yardsticks could be developed by methods long established in the insurance industry. Variables such as the cost of replacing a ship’s control panel are already ‘known knowns’ from the hull portfolio, and can be replicated across the sector.

Where the decision is taken to write cyber as part of a marine book, another problem is getting the wording right. The old Institute Clause CL380, introduced in 2003, specifically excluded cyber risk and was widely derided as hopelessly out of date in the modern world.

In 2019, it was replaced with the Lloyd’s Market Association’s LMA5402, also a blanket exclusion clause, and LMA5403, which covers non-malicious cyber risk but excludes malicious cyber attacks.

There is a body of opinion that neither marks much of a step forward. It is difficult to point to a cyber attack that does not involve an element of malice somewhere down the line.

Some also feel that LMA5403 does not define either ‘malice’ or ‘harm’ sufficiently sharply, which is a signal drawback for a clause of this type.

The International Underwriting Association approach is to look at whether the loss was directly or indirectly caused.

“I think the LMA approach is being preferred in the market for those who want to write non-malicious cyber, though of course this would still leave you without cover for malicious cyber, which is effectively war or terrorism,” pointed out a lawyer at a London law firm specialising in marine insurance.

Even with specialist products, some question the appropriateness of the limits available. Typically,

limits for broad-based cover remain at around $5m or $10m, and going higher than that limits the range of insured risks.

“There’s another way of looking at this,” argues Mr Cooper. “Hull has traditionally bought full value insurance. But even within hull insurance, you have the main hull product and then you have the IV [increased value] product.”

Hull insurance typically covers up to 65%-75% of value, and owners buy IV as a bolt-on in the event of total loss. That is low probability and therefore priced accordingly. More than 90% of hull claims are of less than $10m for attritional losses.

“People don’t need high-value limits. We know other insurers can offer higher limits, but they offer very little cover,” said Mr Cooper. “The cost of paying for a loss, whether it is caused by a hull or a cyber event, will be the same. We know that the loss value is unlikely to breach $10m for a single vessel.”

People want higher limits, without a doubt, he added. However, until a couple of years ago, shipping company insurance budgets were not even taking cyber into account.

Hull, P&I, combined general liability cover and directors’ and officers’ cover are mandatory, and getting more expensive. Cyber remains optional, and is a new product.

So for now, the uneasy compromise remains between owners crossing their fingers, those taking the basic cover and those going for the full package. The market is yet to settle on which strategy will prevail.

The modern three Rs: Ransomware, recommendations and regulation

HIGH-PROFILE cases of cyber attack on some of the shipping industry’s largest companies have raised awareness of the potential impact of cyber crime and the need for both up-to-date security systems and emergency planning procedures, *writes Hill Dickinson’s Mark Weston, who specialises in digital crime.*

Merchant shipping is increasingly reliant on the transfer of data from ship to shore, particularly to monitor vessel efficiency and to demonstrate compliance with increasing global environmental regulations.

However, the digital connections between a ship and its owner can become a weak link if cyber security is not considered.

The risks are numerous, ranging from the infection of operating systems by malware introduced accidentally via a crew member’s laptop or internet link, to deliberate attacks that seek to compromise a vessel’s data or disable its operations.

These risks led to the introduction of comprehensive cyber-security recommendations last year by the International Maritime Organization.

This action has raised awareness of the potential risks that need to be mitigated — but the maritime industry still lags behind many of its land-based compatriots when it comes to understanding the cyber sphere.

The wider world has, unfortunately, come to know the top five cyber risks: ransomware, phishing, data leakage, hacking and insider threats.

There are many others and they have become part of business risk assessments worldwide. If you do not know what any of these are, you should be popping the terms into your nearest online search engine.

Gradually, many businesses in other sectors are implementing various standards regarding IT and information security designed to allow method, policy and process routes to attempt to stop — or, at the very least, reduce the risk of — all of these five threats.

For example, ISO/IEC 27001:2013 (usually better known as ISO27001) is the international standard that sets out the specification for an information security management system.

It uses a best-practice approach aimed to help organisations manage information security by addressing people and processes as well as technology. There are others, too.

The pandemic has shone a light on the role of digital systems to enable business continuity and the importance of back-up systems with robust cyber security.

Today’s maritime sector is particularly prone to attack as technology becomes ever more widely used

and data — whether it is about cargo, staff, location, weather or vessel monitoring — becomes increasingly important and transportable, and able to be corrupted, exploited or stolen if in the wrong hands.

Identifying risk is a sobering exercise. Think about the potential to hack or intercept the remote signal between a vessel and its office; the risks to vessel safety of someone interfering with GPS co-ordinates; the risks to environmental compliance or performance monitoring of a cyber criminal gaining access to vessel sensors and corrupting them or triggering false alarms.

In 2020, the United States Maritime Transportation System, in association with the Information Sharing and Analysis Center, issued its first-ever general warning to all tug owners, advising that their connected operations were vulnerable to cyber attacks — whether they be state-funded hacks, malware hits, virus infections or any of the other myriad cyber threats out there.

That warning was prompted by a phishing email, which was sent to a maritime facility, that had a voicemail attached, imitating a vessel operator. Fortuitously, this was caught and notified to an agency dealing with cyber threats who then alerted MTS-ISAC.

After analysis, the report found that one of the HTTP requests in the email was too sophisticated to be flagged by any known threat detection solution.

There were other sophisticated hallmarks, perhaps too technical to go into here — but suffice to say, it involved an IP address geo-located to Germany.

Those aware of growing dangers to the maritime world will know that the IMO's Facilitation Committee and the Maritime Safety Committee approved new guidelines on maritime cyber-risk management that superseded interim guidelines that had been in place.

Coming into effect in January 2021, these guidelines provide high-level recommendations on maritime cyber-risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities, and include functional elements.

For development and implementation of specific shipping risk management processes and systems, the guidelines are intended to be supplemented by requirements of specific member governments and flag administrations, as well as relevant international and industry standards and best practices.

Many of these are yet to be published; as we know, shipping is often a late-adopter when it comes to technology and regulations.

However, every organisation in the shipping industry is different and the guidelines are expressed in broad terms to have a widespread application; the more complex an entity or its systems, the more care and resources are expected to be expended.

Yet a shipping business does not want to be the most secure, compliant — and insolvent — entity in existence. As with so many areas of law, compliance and regulation, it is about reasonableness and proportionality. The guidelines are recommendatory only — but there is a sting in the tail (more of that later).

The guidelines contain a non-exhaustive list of vulnerable systems, including bridge systems; cargo-handling and management systems; propulsion and machinery management and power control systems; access control systems; passenger servicing and management systems; passenger-facing public networks; administrative and crew welfare systems; and communication systems.

They also make the important distinction between information technology systems (which focus on the use of data as information); operational technology systems (where that data is used to control or monitor physical processes); and interfaces that allow exchange of information within and between such systems.

They also note possible vulnerabilities at every stage of the acquisition and implementation chain, from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber discipline.

That latter issue is often direct (for example, weak passwords allowing unauthorised access) or indirect (such as the absence of network segregation). All these have implications for security and the integrity, confidentiality and availability of information.

Most important of all, these have implications for safety — particularly where critical operations, such as main propulsion systems or bridge navigation, are compromised.

The lack of mandatory status is because a mandatory set of rules would be out of date extremely quickly as technology changes and as new threats develop. Accordingly, the approach taken by the IMO is — as in so many other industries — a resilient and evolving risk-management approach to cyber risks, which is a natural extension of existing safety and security management practices.

One of the biggest issues in cyber-risk management is ensuring that management appreciates the importance of it and is willing to expend resources (read 'cash') to put the necessary preventative measures in place.

This can often be perceived as spending money to stand still — but in reality, it is about mitigating risk so everyone can sleep at night (on the high seas or otherwise)!

The guidelines reflect this by making clear that: "Effective cyber-risk management should start at the senior management level. Senior management should embed a culture of cyber-risk awareness into all levels of an organisation and ensure a holistic and flexible cyber-risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms."

It comes down to the oft-quoted compliance refrain of policies, procedures and process. A key part of this is appropriate training at all levels of the business; everyone has a responsibility for security.

So, for those who have not yet embraced the IMO guidelines, where should a maritime business start?

The guidelines do not spell it out as clearly as I am about to, but any compliance plan should start with the creation of a snapshot as to where an organisation is at; then a plan for where it needs to get to; and the gap is then plugged with a costed, detailed remediation plan.

The plan should be RAG-coded so resources are spent on the 'red' areas first before moving to 'amber' and then 'green'.

The non-sequential functional elements suggested by the guidelines are:

Identify: The need to define personnel roles and responsibilities for cyber-risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

Protect: The need to implement risk-control processes and measures, and contingency planning to protect against a cyber event and ensure continuity of shipping operations.

Detect: The need to develop and implement activities necessary to detect a cyber event in a timely manner.

Respond: The need to develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber event.

Recover: The need to identify measures to back up and restore cyber systems necessary for shipping operations impacted by a cyber event.

And what about that sting in the tail that I mentioned? Despite the guidelines only being recommendations, since January 1, 2021, by Resolution MSC 428(98), the IMO has required cyber security and risks related to be tested in audits; essentially, an organisation must demonstrate that cyber security is an integral part of the safety management systems being used.

In short, it is important to:

• Identify objectives in the field of cyber security;

• Undertake a mapping exercise of existing systems, software, policies, procedures and processes;

• Undertake a gap analysis of the differential between where the current map shows you are and where you need to be in terms of your objectives. This gap analysis then needs to be turned into a costed and step-by-step remedial plan. This will probably include:

Ensuring management buy-in and allocation of key roles and responsibilities for cyber security all the way to management level;

Putting in place or upgrading cyber-security policies and procedures. These need to be workable and used and not just a tick-box exercise or "something you have to have";

Upgrading networks, segregating and hardening them;

Training, training, training of everyone in the organisation, appropriate to their level. This should be both general awareness training and more specific role-based training; and

Implementing hardened systems and network segregation.

Finally, it is vital to ensure that there is also a rolling programme of ongoing compliance and ongoing training so that cyber security is not just "something we checked" but becomes part of "business as usual".

Cyber threats are evolving — and so should you!

MARKETS:

San Pedro Bay ship queues set to increase again

THE number of containerships queuing for berths at Los Angeles and Long Beach has fallen sharply since its peak earlier this year, but there are warnings that the situation could soon reverse and return to levels on par with its earlier high point.

The number of vessels in the Los Angeles and Long Beach queue rose to 66 on February 25, according to figures from the Marine Exchange of Southern California. That was up from 60 a day earlier, but below the peak of 109 on January 9.

But while the fall in numbers has been hailed as a sign of improving productivity at the ports' terminals, a new analysis suggests that reduction has more to do with the number of vessels leaving Asian ports than any major change in the situation in the US.

Figures from Sea-Intelligence's Trade Capacity Outlook show that the steady flow of departures from Asia throughout the fourth quarter of 2021 began took a sharp downturn in mid-January, which after a two and a half week sailing time led to the fall in arrivals and vessels queuing in February.

Moreover, this was not driven by the usual seasonality of Chinese New Year, which this year fell on February 1.

"The only reasonable explanation for this counter-seasonal development will be that the carriers quite simply did not have sufficient vessels available, as those were still stuck in the queues on the other side of the Pacific Ocean," said Sea-Intelligence chief executive Alan Murphy.

But he warned that the dip in vessel departures from Asia was about to come to an end.

"According to the current schedules published by the carriers, the decline will come to an end within the next week, and we are heading into a period where the number of vessel arrivals will begin to significantly exceed the flow in the fourth quarter of 2021.

The maximum reduction in ships queuing would be the first week of March, but by projecting forward from the baseline in the fourth quarter of 2021, Sea-Intelligence warned that the queue could theoretically grow to 120 vessels.

"What is more worrying, is that the data would therefore also imply that if there are no other changes, then the queue will be 25 vessels larger than the baseline, by the end of May 2022," Mr Murphy said.

"The baseline itself, in keeping with the queue growth in the fourth quarter, would imply a queue of 145 vessels. Adding the additional 25 would bring the queue to 170 vessels."

That, however, was unlikely to happen, simply because there were not that many vessels available, he added.

"What will happen instead, is that the sheer shortage of vessels due to them being stuck in a queue, will lead to many more blank sailings than currently shown in the carriers' sailing schedules."

While the shortage of vessels would likely prevent a surge towards even higher numbers, it was clear that the decline in ship waiting was as much due to falling departure numbers as anything else.

"Part of the queue reduction can be caused by improved productivity in Los Angeles and Long Beach, but the numbers here do not show whether or not that is the case," he said. "The numbers do clearly show that such a potential improvement will — up until now — at best be a minor effect, compared to the effect of fewer vessel departures. That also implies that market participants should expect the queue to potentially grow again, as we get into March."

IN OTHER NEWS:

US turns antitrust focus on ocean carriers
THE US Federal Maritime Commission and the Department of Justice have reaffirmed a co-operation agreement following President Joe Biden's push to promote "a fair, open and competitive" domestic market.

FMC chairman Dan Maffei and US Attorney General Merrick Garland announced new steps their respective agencies will take to build last year's agreement to facilitate the exchange of information "between and among attorneys, economists, and technical experts" with especial attention to the Shipping Act.

It follows the recent announcement of a joint international investigation of potential supply chain profiteering by the US, Britain, New Zealand, Australia and Canada.

Suez Canal to raise transit fees by up to 10%
THE Suez Canal Authority has pushed through a set of toll increases that will see transit fees rise by between 5% and 10% for most vessel types.

Bulk carriers, and oil and product tankers will pay an additional 5% on both northbound and southbound legs from March 1.

LNG carriers, along with general cargoships, multipurpose, heavylift and ro-ro ships will be hit with a 7% increase.

CULines orders 7,000 teu pair to expand longhaul operations
CHINA United Lines, an emerging carrier on transpacific and Asia-Europe services, has ordered a pair of scrubber-fitted 7,000 teu containerships, the largest size in its fleet.

The company, also known as CULines, said the order, scheduled for delivery by Shanghai Waigaoqiao Shipbuilding in the second half of 2024, indicates its "long-term planning" to operate the medium to long-haul trade.

Financial details were not disclosed, but brokers priced the eco-designed newbuildings at about $85m each

Maritime safety culture adviser gets investment for expansion
A SAFETY specialist which has advised leading shipping companies on how to avoid accidents has won key funding to expand its business.

SAYFR, a Norway-based specialist in safety culture, has received an investment of Nkr25m ($2.8m) from Corinthian Venture Partners, a Nordic investment fund.

The move follows increased demand for a deeper understanding of organisational culture and the role it plays in safer operations.

Seaspan confirms order for LNG bunker vessels
SEASPAN ULC has placed an order for up to three liquefied natural gas bunker vessels in China.

Hong Kong-listed CIMC Enric said its subsidiary yard Nantong CIMC Sinopacific Offshore & Engineering has been contracted for the two firm 7,600 cu m ships plus an option for one more.

Financial details of the newbuildings, designed by Vard Marine, were not disclosed.

Yangzijiang to become 'pure-play shipbuilder' with investment arm spinoff
YANGZIJIANG Shipbuilding, a privately run shipbuilder, will spin off its debt investment segment to concentrate on its core business.

The move will see the China-based, Singapore-listed company become a "pure-play" shipbuilder, it said in a stock exchange statement.

"This spin-off will allow the group to focus on its core shipbuilding business, strengthening its corporate governance by accelerating its [environmental, social and corporate governance] repositioning," it said.

Classified notices follow