



Law around cyber attacks still raises more questions than answers

By admin On September 17, 2021 In Cargo, Insurance Marine News, Keep, Legal, Marine Hull, Marine Liability

A cyber-attack scenario on a container ship calling at a port illustrated two plain facts, that there are a large number of contracts between the various interested parties, and that the answers to the legal questions surrounding cyber-attacks remains untested and, usually uncertain.

Those, and the fact that the cyber threat in the maritime industry is real, significant, and already happening, were the key takeaways from yesterday's Quadrant Chambers breakfast briefing, held at 10 Fleet Street as part of London International Shipping Week.

Paul Dean, global head of marine at legal firm HFW, joined three Queens Counsel from Quadrant Chambers – James M Turner, Nichola Warrender and Nigel Cooper. Laying the ground, Turner observed that container ships were no strangers to headlines at the moment. There was congestion at many ports around the world. There were container shortages, Covid-19 related concerns, delays at many ports and, the subject of yesterday's briefing, cyber-attacks. Turner said that events in the container shipping sector were having real-world consequences that were visible to all. Rates had been going through the roof, but still it seemed that demand on the major routes into the US and Europe were full up.

Paul Dean from HFW then outlined some of the risks of cyber. He recounted the NotPetya attack on Maersk, and the less headline-grabbing but no less important disruptions at CMA CGM (two weeks) and even at the International Maritime Organization (one week). Dean said that there was an average of one incident a day on board international ships, but that a large proportion of these are not reported. He also observed that there was a new victim of a ransomware attack every 10 seconds. Attacks on shipping rose 900% over the three years to 2020. Meanwhile, ethical hackers had shown how it was possible to take control of the bridge of a ship.

Dean said that the risks to containership were more profound when compared to other tonnage. He also noted, in passing, that what happened to the vehicle

carrier **Golden Ray** could easily happen again as a result, not of human error in ballast requirement estimation, but because of a cyber-attack.

Looking at the topic of seaworthiness, Dean said that cyber was an aspect of this. He did not think that the International Ship and Port Facility Security (ISPS) in its current form was sufficient. He noted that it was developed to enhance the security of ships and port facilities in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the US. Dean observed that technology had moved on considerably since 2001.

Dan also felt that the rules around compliance (see IMO MSC.428 (98)) were not on their own enough. By comparison, he said that a vessel could be in class, but that did not prove that it was currently seaworthy.

Dean said that the solutions were at the front end and back end.

There needed to be a wide-ranging cyber security review, covering commercial, operational. Technical, compliance, legal and insurance. Parties needed to be looking at their supply contracts, he said.

Dean also covered a topic that many in the industry mention when it comes to cyber threats – that being the danger inherent in the links between operation technology and information technology. There were hybrid systems on containerhips, and the danger was that an attack via one sector could result in a disablement in both.

On board cyber security monitoring, which is one of the things that Cyberowl (with which HFW has set up a cooperation agreement) do.

Finally, Dean mentioned another theme common in risk management circles in the marine sector. Not only do you need to try to prevent something wrong, but you need to train for what to do if something does go wrong. Preparations in case of a cyber breach make people far more likely to act correctly if a breach takes place.

This brought Nigel Cooper QC onto a scenario that he put together, with several interested parties.

These were:

- High-speed liner service operated by Containers 4 U, which was bringing ship...
- ... **Lotsa Stuff**, a 20,000 teu ULCV, into ...
- ... Port A.
- Lotsa Stuff was owned by Big Investments Ltd. It was leased on a bare bone charter to ...
- ... Bare Boat Ltd (Demise), which in turn time-chartered it to Containers 4 U, which had an agreement with associated party ...
- ... Boxes R Us.

None of the contracts between the various parties incorporated the BIMCO 2019 cyber security clause.

When an engineer came on board he connected his computer to the cargo handling computer, and gave the chief officer a USB stick, which was put into the business computer so that it could be linked to a printer.

The Master was then informed by port authorities that he is about to be subject to a PSC. He tells the terminal of this fact by email.

A short while after the IT systems freeze and a ransomware note is received. Cargo handling systems at the port have also collapsed as the port has been affected by the cyber-attack as well. The PSC detained the vessel at berth. By this time the terminal's computers were down, and all onshore automation has failed. In effect, containers can't be moved.

It was noted that the terminal had received four similar ransom notes in the previous month.

By now there are ships waiting outside for the berth to become available, with more arriving all the time.

Where does the blame lie? The owners and bareboat charterer are blaming C4U. The terminal is blaming the vessel for infecting and crashing its systems via the email sent by the master. Boxes R Us is blaming C4U and is demanding alternative arrangements for discharge.

There's no time frame fixed for when it will end.

Nichola Warrender QC then looked in detail at the contracts. She noted that there were many of these to consider, even when one restricted oneself to internal contracts.

There was the bareboat/demise charterparty contract between the owner and the bareboat charterer. There was the time charter contract between the bareboat charterer and the time charterer. There was the vessel sharing agreement (slot charter) contract between the time charterer and the slot charterer, and then there were the Bills of Lading and contracts of carriage between the slot charterer and the container owners / owners of the goods in the containers.

Warrender also noted that some parties played a dual role, looking to protect other interests both up and down the chain. The form of the contracts would differ in form in each tier. So the manner in which cyber breaches were dealt with were different, as were the agreements on how such disputes would be resolved.

Finally, at the end of the sequence, one had the containers themselves, which on ULCVs would be subject to the contract of the one of the many container lines

having containers on the vessel/ Warrender said that one of the most complex aspects was how cargo on board could be the subject of widely varying conditions – a point averred to later by Nigel Cooper when he commented that it could take a decade to establish where the liability for cargo losses lay (and how much they were), even before one moved on to dealing with how such losses might be allocated to liability insurers.

In this scenario the goods had not (yet) suffered loss or damage. Warrender noted that the Hague and Hague Visby do not touch the concept of delay. She noted that, in terms of delay, the risk was stacked against the ordinary holder of a bill of lading (BoL).

VSA contracts were bespoke, so it would depend on the precise terms of the agreement. The VSA contract would often be between parties that were either related or part of long-term alliances. So what is desired is that time charterer compensates the VSA partners and then passes its expenditure up the contract chain. In terms of delay, although the VSA might be confident that it can win, that did not mean they did not have exposure. Legal fees, demurrage, mislocation, and reputational damage were all matters of concern, particularly if one claimed to be a high-speed liner.

Warrender said that between such parties it was likely that there would be an agreement to deal with losses, but she said that she had yet to come across an agreement that detailed what would happen in the case of cyber losses. “So I would say Watch This Space”.

In this scenario the time charter took the standard form of NYPE (New York Produce Exchange Form), but it would be likely that there would be some contractual changes to mitigate the exposure of the bareboat charterer. Warrender said that often one saw bespoke offhire provisions. Once again, Warrender said that she had not yet seen a bespoke amendment that dealt with cyber, but she did not see why there should not be one.

As had been noted elsewhere this week in LISW 2021, the BIMCO Cyber Security Clause 2019 had two interesting clauses which many lawyers thought could cause some problems down the line. These were clauses ‘b’ and ‘d’, with the former using the term “reasonable endeavours” as a requirement to ensure that any third-party providing services on its behalf complies with terms of clauses as a (i) to a (iii) (which refer to the implementation of “appropriate” cyber security systems). Meanwhile clause ‘d’ has as a default liability for a breach or series of breaches of the cyber security clause of just \$100,000. Although there is a blank amount that can be filled in to amend this, by the nature of things lawyers feared that most signatories would take the default, and this could turn out to be rather a low sum.

Warrender then observed that interests clearly went beyond the internal interests mentioned above. There were, for example:

- Port/terminal operators
- their port users (waiting vessels)
- insurers
- other users of the liner service.

The sheer number of other users that could be affected was something unique to container vessels.

James Turner then approached the unsafe port angle, looking at how liability might be apportioned in a legal case. Justice Sellers ruling in the 1958 *Eastern City* case, a ruling given only two years after the completion of the first container shipment, One notes that the UK Defence Club's pdf on the matter of the law relating to unsafe ports starts with the Sellers definition:

"A port will not be safe unless, in the relevant period of time, the particular ship can reach it, use it and return from it without, in the absence of some abnormal occurrence, being exposed to danger which cannot be avoided by good navigation and seamanship..."

Turner then asked the question: What was the danger that the ship was exposed to? After all, a ship was exposed to a cyber-attack anywhere. Was there an enhanced risk and, if so, by reference to what feature of the port? It is here that the point that the port had suffered four "similar" incidents in the previous month might turn out to be a matter of legal significance. Turner said that the aim for the owners would be to "set up the cyber equivalent of the uncharted reef".

Here Turner noted another unfortunate consequence for the owners. While they would be attempting to defend themselves against charterers passing liability up the chain, the ports would like be unwilling to make such details available. He cited the *Ocean Victory* case, on which the UK Supreme Court ruled in May 2017 on three important issues: safe port obligations in charter parties, the impact of insurance provisions on the right to claim against third parties, and the scope of limitation of liability. Turner said that in this case it had proved difficult to extract information from the port as to the accuracy of the ruling that the danger of storms closing the entrance/exit to the port were "characteristics" of the port in question.

In a cyber case, factual evidence would be crucial in establishing a relevant danger to which the vessel was exposed. Could this have been avoided by good seamanship? Is reasonable cyber security a facet of this? Turner said that "I think we can be quietly confident that now that it is".

The matter I question here is that a clause allocates risk of an unsafe port to the charterer, which presupposes that those risks can't be avoided. However, Turner said that it was important not to lose sight of the "abnormal occurrence" for which charterers do not need to take the risk.

In the event of a claim that a port was “unsafe” because of the cyber risk, Turner said that he did not think that an unsafe port claim was inconceivable, but he did feel that it would face considerable legal challenges.

Nigel Cooper then looked at the insurance aspect.

He said that the fallout of such a cyber event could be huge in terms of cost and the time required. Much of that burden would be borne by the different insurance interests, but the three major problems were identifying those interests, identifying the degree of loss, and then allocating the liability for that loss.

In this scenario, Cooper noted that the container line that might have its own onward distribution service and its own cargo handling operation, with a sequence of policies with clauses related to double insurance, exclusions related to other covers, and so on. You could even have a situation where the container line doesn’t know what policies it has or what its levels of cover actually are.

Cooper said that the first risk to containers in this case was one of delay. After that there could be a risk of physical damage to perishables.

This would fall to the cargo insurers. After paying the claim, they could try to reclaim the loss from liability insurers.

There were also the terminal interests. The insurers of the port operator and the insurers of the cargo handler were likely to be property and liability insurers.

For the vessel itself one would immediately think P&I cover, but there were situations where one could also be looking at hull and machinery cover. “In our scenario it looks like it will be the demise party whose claims will be engaged”, Cooper said.

Boxes R Us liability insurance could also enter the scenario, he said. Depending on the onward carriage arrangements, freight forwarders insurers could also appear.

Finally, the liability insurers of the engineer’s employers (it was the engineer who handed over the USB which the Captain inserted into the computer system) and the limits on liability on his cover.

That, however dealt only with the interests of those directly engaged. In this scenario there were also vessels offshore that were being delayed. All of the interests on all of these vessels would also have insurers, all of whom might receive claim from their customers/members and all of whom might then seek to reclaim those payments from the first-party insurers.

Finally there was a possibility that, with the software systems of the port going down, that containers might go missing. Alternatively, they might be misdirected,

ending up thousands of miles away from where they should be. That would entail a cost of return or, possibly a write off of the contents.

With the increasingly high cost of automated equipment in ports, the cost of damage to terminal equipment and infrastructure would also be claimed from somewhere.

Then there was business interruption. If that BI cover is linked to loss or damage to physical assets, has that damage occurred? Cooper referred here to the recent ruling on FCA vs Arch, which related to the nature of Covid-19 and whether businesses could claim from their BI insurers.

Did cyber qualify as a “physical obstruction” to leaving the berth?

Cooper observed that, given the scope of likely third-party claims it could be difficult to keep the claims to one jurisdiction, or indeed to one body of law. One would be dealing with huge schedules, and it would take a considerable time simply to decide what claim was where.

It was noted that the P&I Clubs did not exclude cyber cover, subject to a war or terrorist exclusion. However, this raised the possibility of a complexity when it came to deciding whether there was a war or terrorist aspect. As one audience member observed, this was made more complex by the fact that most ransom demands were in the form of crypto currency, which made identifying the source (and location) of the demand difficult to ascertain. Given OFAC’s position on payment of ransom to sanctioned organizations, this could make matters more complex, as even P&I Clubs tell insureds that payments of ransoms to terrorist organizations would not be covered.

It was also observed by Cooper that, as yet, there was no standard definition of a cyber-attack. It was more of a case of knowing it when you saw it. However, the lack of a standard clause meant that the problem of establishing a causative link (see FCA vs Arch, above) had no directly applicable case law and little to go on in terms of what was written in contracts.

One example raised by Cooper was hackers accessing the data of a shipping company, and then doing nothing more with the insureds system, but using the data obtained to hack other systems, attacking third parties. Would that be defined as a cyber risk?

Another question asked by Cooper was, “What is the nature of the insured risk?” If the insured does not have adequate protocols, is that a failure in the terms of the insured services or a failure within the structure? Cooper observed that he was not answering many of these questions. He said that the reason for that was that many of the questions were currently “live”.

What we haven't yet seen are specific loss prevention clauses in policies that deal with the protocols to be in place as part of cyber security. Most policies have general loss prevention clauses complying with use of best endeavours to reduce or avoid risk. Could these be used to limit or exclude cover? On the face of it, they could, said Cooper.

The final "big" question related to General Average. While there was some guidance by referring to traditional piracy, this moved one into completely untested areas. For example, if the ship were immobilized, and a computer expert came in from a third-party company and managed to unfreeze it, could that be deemed "cyber salvage"? Turner thought that the answer to this was, probably, Yes.

But GA was more difficult. When a ship has been taken over by pirates then it has been accepted for some years that a ransom is payable by cargo interests. But the focus of GA has been on physical risk. As had been observed by Justice Teare, the level and type of danger required to trigger a GA claim is different from that for triggering salvage claims. Was the Maritime adventure sufficiently imperilled?

Turner said that this would be an interesting and difficult thing to decide. His hunch was that it was a real danger, rather than the metaphorical equivalent of a ship just being stuck. It's more threatening than that.

However, this led to the inevitable question. If there the concept of cyber salvage was accepted, then which insurer would pay it? Cooper said that we would all be engaged for a very long time working that one out. He said that it was hard to see it as falling on the property insurer, but in this scenario which liability insurer it would fall on was harder to establish. "It could be a question of whose exclusions are more effective", he said.

Finally, returning to the start of the story – the USB stick. It was generally accepted that taking a USB stick from a third party and inserting it into the ship's network was negligent on the part of the captain. But if it came to court the question would be "was it causative". Given that the systems went down, proving conclusively that the cause was the USB stick could be harder. Until the systems were unlocked it would be hard to establish.

Wrapping up. Paul Dean said we all recognized that cyber risk was real, was here now, and that regulations and the law generally had to catch up with the new technology.