HILL DICKINSON

SHUTTING THE STABLE DOOR

AFTER THE CYBER HORSE HAS BOLTED

Julian Clark, Global Head of Shipping, Hill Dickinson;
Donal Keaney, Marine Manager, Hill Dickinson, London, UK

As we reach the end of 2017 it seems that every other article and maritime presentation is in some way linked to cyber risk. New guidelines issued by both BIMCO and the IMO aim to give guidance on how security measures can be improved and from 2021 cyber security will form part of the ISM Code opening up the cyber elements of port state control.

But cyber risk in shipping and in relation to port security has been with us for some time, as the following incident highlights.

THE CASE OF THE VANISHING CONTAINER

In 2011 the Port of Antwerp introduced an electronic release system (ERS), intended to replace the existing system for the authorization of cargo release, through delivery orders or release notes.

The system was not mandatory, but was embraced by a number of carriers using the port. These carriers would send computer-generated pin codes via email to cargo receivers or their agents, as well as the port terminal.

It was subsequently found that containers had been removed by a sophisticated criminal gang, who were using the containers for the illicit carriage of drugs. It later transpired that the gang had retained the services of computer hackers to gain access to the IT infrastructure of receivers' agents, over a number of years. In this way the gangs had been able to access data showing the location and security details of containers so that drugs could be removed prior to the delivery of the container to its rightful owner. Containers could also be moved round the port in order to facilitate access for the gangs.

It is now believed that the process had been on-going for a number of years prior to detection and that initially access to the systems had been gained via virus (RAT – remote access technology) software emailed to staff, and then subsequently by introducing key logging devices following a break-in in order to frustrate the introduction of higher security firewalls.

Ultimately the hackers were used to obtain the pin codes required in order to take delivery of the containers at the Port of Antwerp. It was this development, leading to the theft and absence of whole containers, which brought the whole incident to light. The process has been described as, "a new business model of organised crime activity".

THE LAW CLOSES THE STABLE DOOR

The ERS system was adopted by the container carrier, Mediterranean Shipping Company (MSC), and utilised for the carriage and delivery of 69 consignments on behalf of the shippers, Glencore.

Upon receipt of the relevant pin codes by email, Glencore's agent presented at the port to collect the containers. However it was found that two containers due for

collection had already been removed from the port.

Glencore sued MSC under UK jurisdiction, claiming damages for breach of contract, the base for its claim being that the cargo should have been delivered against bills of lading, not the presentation of a pin code.

At first instance, the English High Court found in favour of Glencore, a decision that was appealed by MSC on five grounds:

1. The provision of pin codes constituted a symbolic delivery of the goods. MSC argued that the delivery of the pin codes amounted in law to the delivery of possession of the goods, likening it to the delivery of a key to a warehouse where goods were stored.
2. The email containing the pin codes was in itself a delivery order for the purposes of the bill of lading. MSC relied on the absence of a definition of "delivery order" on the bill of lading to contend that a delivery order was capable of having different meanings.
3. The email containing the pin codes constituted a ship's delivery order, within section 1(4) of the Carriage of Goods by Sea Act 1992 in the UK, and that it represented an undertaking by MSC to deliver the goods to whoever first produced the pin.
4. Estoppel. MSC argued that Glencore was estopped from contending that the use of the ERS was in breach of contract because Glencore had accepted this system for the previous shipments.
5. In an application to adduce new evidence, MSC argued that it was the IT systems of the receiver's agents which allowed the hackers to obtain the pin codes, thereby breaking the chain of causation.

The Court of Appeal was not satisfied with any of the grounds on which the appeal was based, and it was dismissed leaving the innocent MSC carrying the can and bearing the loss.

PAST CONTAINER CARGO THEFTS

The theft of cargo using falsified or stolen documents is not new. In the past, criminals have obtained information on the contents of containers from employees of shippers, receivers or carriers, often through bribery or blackmail.

Once a container with desirable contents had been identified, the criminals would either steal the required documents, or produce elaborate forgeries, in order to convince those responsible for port security that they were the party entitled to remove the container from the port. Often, such cases as those described above would involve the services of a person "on the inside". One of the benefits of digital

shipping documentation is the reduction in manpower required to administer the system which, in turn, reduces the number of persons to which sensitive information, such as pin numbers, is exposed.

Such cases of theft from a port facility exposed port operators to potential claims from customers arising out of the misdelivery of cargo. As such, ports have spent a lot of time and money over the years developing and implementing the necessary safeguards to minimize this exposure.

ANALYSIS

It is apparent that the procedures developed to prevent the more traditional tactics employed by criminals wishing to steal cargo are largely ineffective in preventing theft in the digital age.

The above case provides a good example of the due diligence which must be undertaken before introducing new systems of work that require the participation of third parties. This case involved customers of the port, however, similar problems may have arisen in dealings with suppliers, service providers and trade partners.

It is important to ensure that any new procedures are well documented, and that responsibilities of the parties are clearly set out. When an organization adopts any form of new technology it is vital to consider and implement adequate legal and security measures in advance and before, as the saying goes, "the horse has bolted".

Whenever technology is introduced to replace traditional paper-based systems, it is important for operators to ensure that all elements of the system being replaced are covered in the new system, and that all parties are aware of the relationships between the obsolete paper documents, and the digital article which is replacing them.

The fifth ground for MSC's appeal also highlights the need for due diligence in ensuring that third parties participating in the digitizing of paper-based systems have in place the necessary IT infrastructure and security protocols to minimize the risks of data breach at their end.

ABOUT THE AUTHORS

Julian Clark is global head of shipping at Hill Dickinson with overall responsibility for the casualty, litigation and transactional shipping teams throughout the firm's network of offices. He has over 25 years' experience of litigation, arbitration and mediation and specializes in casualty, marine insurance and charter disputes.

Donal Keaney is marine manager and a master mariner with almost 20 years' experience in the shipping industry. His areas of expertise include marine casualty, salvage, general average, ports and terminals, charterparty and bill of lading disputes.

ABOUT THE ORGANIZATION

Hill Dickinson is an international law firm operating across offices in the UK, mainland Europe and Asia. With strong roots in the shipping industry and more than 100 marine legal experts, the firm delivers advice and strategic guidance spanning the full legal spectrum, from non-contentious advisory work to all forms of dispute resolution.

ENQUIRIES

Emails: julian.clark@hilldickinson.com, donal.keaney@hilldickinson.com