SHIP MANAGEMENT INTERNATIONAL

Issue No 72 March/April 2018

IoM joins the cluster race

Notebook

Watch out, there's a thief about!

Charlotte Kirk (pictured), a director with International Transport Intermediaries Club (ITIC), explains why it may be worthwhile that ship managers review their business systems and controls as a way of minimising the risk of fraud

The increased incidence of fraud – and how to detect, minimise and prevent it – has been the focus of extensive recent discussion in the maritime sector. Cyber-crime has dominated much of the debate, but ship managers should be aware that the problem of fraud is not limited to crimes perpetrated by criminals from outside their organisation gaining access to their systems.

Although securing protection against ransomware and other cyber-threats is of vital importance, this should not blind ship managers to the possibility of frauds perpetrated by individuals within their own organisations.

ITIC has seen a wide variety of frauds, all of which have one thing in common – they involve criminals seeking to extort money. A common feature is for the criminals to arrange for their victims to pay more than they need to, and then keep the difference for themselves.

A simple example was a fraud run for a number of years by an executive in a ship manager's purchasing department. He arranged for goods to be supplied by 'his contacts'. In fact, the invoices came from a company he had created, and were for slightly inflated prices. He ordered the

goods from genuine suppliers, and the suppliers invoiced the address they were given in the correct amount. He then paid them out of the money he had received and pocketed the difference.

Repeated small frauds of this type often add up to significant sums over time and can be difficult to spot. Often it is an unexpected event (in this case a dispute over a defect in the goods supplied) that brings the fraud to light. When the fraudster is exposed, other staff members invariably say that the individual was unusually sensitive about any queries in connection with 'his business', always insisting that he would sort them out himself.

Another fraud seen by ITIC involved an unexpected staff absence leading to the discovery of a fleet manager who was engaged in 'ghost payrolling'. This employee created a fictitious officer whom he 'deployed' on various ships in the managed fleet. The payroll had been outsourced to an external company, and the fleet manager insisted that only he would sign off the crew payrolls – something which, on reflection, the shipmanagement company admitted was strange for someone of his seniority. It did however enable him to arrange payments to the fictitious officer without scrutiny. By deploying 'his officer' across the fleet, the additional costs fell on different owners. Once the fraud was uncovered it was realised that, for a short period, 'his officer' had supposedly been 'working' on two ships in the managed fleet.

Elsewhere, crew payments in cash proved too tempting for an employee of a ship manager in the Far East. An investigation prompted by the discovery of large discrepancies in one of the managed fleet's accounts revealed that one of the crewing team had a very simple scam going on involving the issuing of inflated fund requests for final salaries of seafarers signing off from ships. The fund requests were presented to the accounting team, who issued the salaries in cash.

The crewing executive put the correct amount of cash into sealed envelopes for

a visiting superintendent to pass to the Master of the ship and kept the balance created by the inflated fund request. The superintendent brought back the acknowledgement receipts from the seafarers, whereupon the member of the crewing team recorded the crew as having received the higher amounts and disposed of the actual receipts. Over time, $900,000 had been stolen.

A lesson drawn from these accounting frauds is to be careful to avoid an individual having the ability to control every aspect of a transaction with minimal scrutiny. It may be worth ship managers having a review of the systems and controls in their business to minimise the risk of fraud.

Dunkirk beats 50 million tonnes record

The French port of Dunkirk has announced a small growth in cargo traffic for 2017 to just over 50.4 million tonnes, aided by increases in solid and liquid bulk cargoes.

General cargoes handling was, however, 9% down overall, with a tonnage of 20.55 m tonnes while cross-Channel traffic posted a good year but had to contend with fierce competition from the other operators in this sector. Traffic totalled 16.4 MT, a fall of 10%. The number of trucks and trailers was 11% lower with 612,000 freight units. Passenger numbers dropped 8% to 2.67 million, and passenger vehicles were down by 9% to 699,000. Containers ended the year with a new record of 374,000 TEU and an increase of 10%.

Solid bulk traffic in 2017 was helped by heavy bulks and reached 24.55 m tonnes, an increase of 11%. Grain experienced contrasting results with imports setting a new record with more than 350,000 tonnes and growth of 31%. However, as for all French ports, exports were affected by the very poor harvest in 2016 and the delay in shipments of the 2017 harvest and fell 63% to 950,000 tonnes.

After several difficult years, liquid bulks are benefiting from the opening of the LNG terminal with petroleum products climbing 3% to a tonnage of 3.4 m tonnes.